DATA RECORDER RESTORING ORIGINAL DATA ALLOWED TO EXIST ONLY UNIQUELY

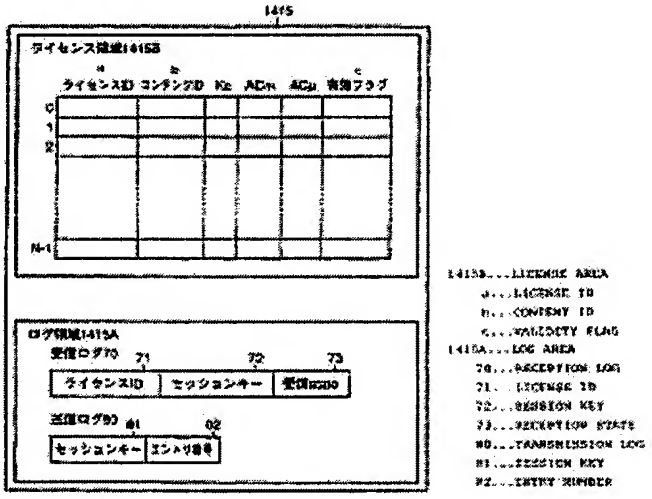
Publication number: WO02075550 (A1)
Publication date: 2002-09-26
Inventor(s): HORI YOSHIHIRO [JP]
Applicant(s): SANYO ELECTRIC CO [JP]; HORI YOSHIHIRO [JP]
Classification:
- international: ***G06F21/00; G07F7/10;*** **G06F21/00; G07F7/10;** (IPC1-7): G06F12/14; G06F15/00; G06F17/60
- European: G06F21/00N1D1; G06F21/00N7D; G06F21/00N7T; G07F7/10D2P; G07F7/10D10M
Application number: WO2001JP07862 20010910
Priority number(s): JP20010073827 20010315

Also published as:
US2004088510 (A1)
JP3696206 (B2)
CN1493030 (A)
CN1324484 (C)

Cited documents:
JP2000305853 (A)
JP2000285028 (A)
JP2001051906 (A)
JP2001014221 (A)
JP2001022859 (A)

Abstract of **WO 02075550 (A1)**

A log area (1415A) and a license area (1415B) are arranged in the memory of a memory card. In the license area (1415B), a license, e.g. a license ID and a license key Kc, and a validity flag, related to the entry number 0 to N-1 are stored. In the log area (1415A), a receiving log (70) and a transmission log (80) are stored. The transmission source of the license, i.e. the memory card, accepts a reception state from a destination memory card and validates the validity flag of an area designated by the entry number of the transmission log (80) if the reception state is on. Consequently, the license which is the object of transfer/duplicate can be restored even if the communication is interrupted during the transfer/duplicate of the license.



(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2002 年9 月26 日 (26.09.2002)

PCT

(10) 国際公開番号
WO 02/075550 A1

(51) 国際特許分類[7]: G06F 12/14, 15/00, 17/60

(21) 国際出願番号: PCT/JP01/07862

(22) 国際出願日: 2001 年9 月10 日 (10.09.2001)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2001-73827 2001 年3 月15 日 (15.03.2001) JP

(71) 出願人 (米国を除く全ての指定国について): 三洋電機株式会社 (SANYO ELECTRIC CO., LTD.) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 Osaka (JP).

(72) 発明者; および

(75) 発明者/出願人 (米国についてのみ): 堀 吉宏 (HORI, Yoshihiro) [JP/JP]; 〒570-8677 大阪府守口市京阪本通2丁目5番5号 三洋電機株式会社内 Osaka (JP).

(74) 代理人: 深見久郎, 外 (FUKAMI, Hisao et al.); 〒530-0054 大阪府大阪市北区南森町2丁目1番29号 三井住友銀行南森町ビル Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

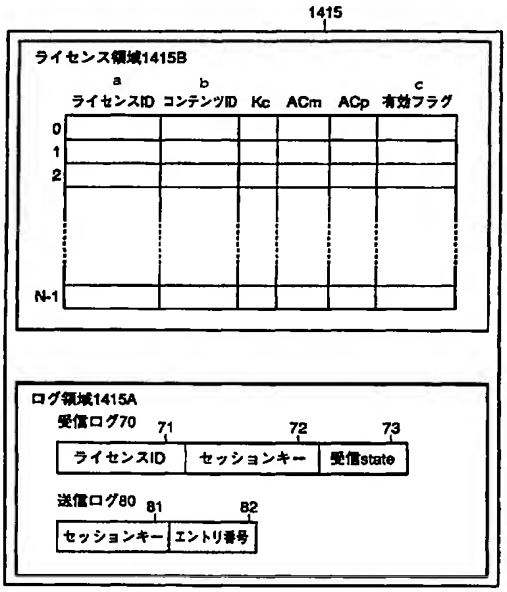
(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書
— 補正書

[続葉有]

(54) Title: DATA RECORDER RESTORING ORIGINAL DATA ALLOWED TO EXIST ONLY UNIQUELY

(54) 発明の名称: 一意義的にのみ存在が許容される独自データを復元可能なデータ記録装置



1415B...LICENSE AREA
a...LICENSE ID
b...CONTENT ID
c...VALIDITY FLAG
1415A...LOG AREA
70...RECEPTION LOG
71...LICENSE ID
72...SESSION KEY
73...RECEPTION STATE
80...TRANSMISSION LOG
81...SESSION KEY
82...ENTRY NUMBER

(57) Abstract: A log area (1415A) and a license area (1415B) are arranged in the memory of a memory card. In the license area (1415B), a license, e.g. a license ID and a license key Kc, and a validity flag, related to the entry number 0 to N-1 are stored. In the log area (1415A), a receiving log (70) and a transmission log (80) are stored. The transmission source of the license, i.e.

[続葉有]

WO 02/075550 A1

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

the memory card, accepts a reception state from a destination memory card and validates the validity flag of an area designated by the entry number of the transmission log (80) if the reception state is on. Consequently, the license which is the object of transfer/duplicate can be restored even if the communication is interrupted during the transfer/duplicate of the license.

(57) 要約:

メモリカードのメモリにはログ領域（１４１５Ａ）とライセンス領域（１４１５Ｂ）とが配置されている。そして、ライセンス領域（１４１５Ｂ）は、ライセンスＩＤおよびライセンス鍵Ｋｃ等のライセンスと有効フラグとをエントリ番号０～Ｎ－１に対応して格納する。ログ領域（１４１５Ａ）は、受信ログ（７０）と送信ログ（８０）を含む。ライセンスの送信元であるメモリカードは、受信先のメモリカードから受信ｓｔａｔｅを受理し、受信ｓｔａｔｅがＯＮであれば、送信ログ（８０）のエントリ番号によって指定された領域の有効フラグを有効にする。その結果、ライセンスの移動／複製の途中で通信が切断されても、移動／複製の対象となったライセンスを復元できる。

明細書

一意義的にのみ存在が許容される独自データを復元可能なデータ記録装置

技術分野

この発明は、コピーされた情報に対する著作権保護を可能とするデータ配信システムを用いて取得された暗号化データを復号および再生するためのライセンス等の一意義的にのみ存在が許容される独自データを他のデータ記録装置へ移動／複製するためのデータ記録装置に関するものである。

背景技術

近年、インターネット等のデジタル情報通信網等の進歩により、携帯電話機等を用いた個人向け端末により、各ユーザが容易にネットワーク情報にアクセスすることが可能となっている。

このようなデジタル情報通信網においては、デジタル信号により情報が伝送される。したがって、たとえば上述のような情報通信網において伝送された音楽や映像データを各個人ユーザがコピーした場合でも、そのようなコピーによる音質や画質の劣化をほとんど生じさせることなく、データのコピーを行なうことが可能である。

したがって、このようなデジタル情報通信網上において音楽データや画像データ等の著作者の権利が存在するコンテンツが伝達される場合、適切な著作権保護のための方策が取られていないと、著しく著作権者の権利が侵害されてしまうおそれがある。

一方で、著作権保護の目的を最優先して、急拡大するデジタル情報通信網を介してコンテンツデータの配信を行なうことができないとすると、基本的には、著作物データの複製に際し一定の著作権料を徴収することが可能な著作権者にとっても、かえって不利益となる。

ここで、上述のようなデジタル情報通信網を介した配信ではなく、デジタルデータを記録した記録媒体を例にとって考えて見ると、通常販売されている音楽デ

ータを記録したＣＤ（コンパクトディスク）については、ＣＤから光磁気ディスク（ＭＤ等）への音楽データのコピーは、当該コピーした音楽を個人的な使用に止める限り原則的には自由に行なうことができる。ただし、デジタル録音等を行なう個人ユーザは、デジタル録音機器自体やＭＤ等の媒体の代金のうちの一定額を間接的に著作権者に対して保証金として支払うことになっている。

しかも、ＣＤからＭＤへデジタル信号である音楽データをコピーした場合、これらの情報がコピー劣化の殆どないデジタルデータであることに鑑み、記録可能なＭＤからさらに他のＭＤに音楽情報をデジタルデータとしてコピーすることは、著作権保護のために機器の構成上できないようになっている。

このような事情からも、音楽データや画像データ等のコンテンツデータをデジタル情報通信網を通じて公衆に配信することは、それ自体が著作権者の公衆送信権による制限を受ける行為であるから、著作権保護のための十分な方策が講じられる必要がある。

この場合、デジタル情報通信網を通じて公衆に送信される著作物である音楽データや画像データ等のコンテンツデータについて、一度受信されたコンテンツデータが、さらに勝手に複製されることを防止することが必要となる。

そこで、コンテンツデータを暗号化した暗号化コンテンツデータを保持する配信サーバが、携帯電話機等の端末装置に装着されたメモリカードに対して端末装置を介して暗号化コンテンツデータを配信するデータ配信システムが提案されている。このデータ配信システムにおいては、予め認証局で認証されたメモリカードの公開暗号鍵とその証明書を暗号化コンテンツデータの配信要求の際に配信サーバへ送信し、配信サーバが認証された証明書を受信したことを確認した上でメモリカードに対して暗号化コンテンツデータと、暗号化コンテンツデータを復号するためのライセンス鍵を送信する。そして、ライセンス鍵を配信する際、配信サーバおよびメモリカードは、配信毎に異なるセッションキーを発生させ、その発生させたセッションキーによって公開暗号鍵の暗号化を行ない、配信サーバ、メモリカード相互間で鍵の交換を行なう。

最終的に、配信サーバは、メモリカード個々の公開暗号鍵によって暗号化され、さらにセッションキーによって暗号化したライセンスと、暗号化コンテンツ

データとをメモリカードに送信する。そして、メモリカードは、受信したライセンス鍵と暗号化コンテンツデータとをメモリカードに記録する。

そして、メモリカードに記録した暗号化コンテンツデータを再生するときは、メモリカードを携帯電話機に装着する。携帯電話機は、通常の電話機能の他にメモリカードからの暗号化コンテンツデータを復号し、かつ、再生して外部へ出力するための専用回路も有する。

このように、携帯電話機のユーザは、携帯電話機を用いて暗号化コンテンツデータを配信サーバから受信し、その暗号化コンテンツデータを再生することができる。

一方、インターネットを用いて暗号化コンテンツデータをパーソナルコンピュータに配信することも行なわれている。そして、パーソナルコンピュータへの暗号化コンテンツデータの配信においては、パーソナルコンピュータにインストールされたソフトウエアによって暗号化コンテンツデータの配信が行なわれており、暗号化コンテンツデータに対するセキュリティは、暗号化コンテンツデータをメモリカードに書込む場合より低い。また、上記のメモリカードと同じセキュリティを持つデバイスをパーソナルコンピュータに装着すれば、上記の携帯電話機に対する暗号化コンテンツデータの配信と同じ配信をパーソナルコンピュータに対して行なうことが可能である。

そうすると、パーソナルコンピュータは、インストールされたソフトウエアと、上記デバイスとによって暗号化コンテンツデータを受信する。つまり、パーソナルコンピュータは、セキュリティレベルの異なる暗号化コンテンツデータを受信する。

さらに、音楽データが記録された音楽ＣＤが広く普及しており、この音楽ＣＤから音楽データをリッピングによって取得することも行なわれている。そして、このリッピングによって音楽データから暗号化音楽データ（暗号化コンテンツデータ）と、その暗号化音楽データを復号して再生するためのライセンスとが生成される。そして、このリッピングにおいては、コンテンツデータの利用規則を規定するウォータマークをコンテンツデータから検出し、その検出したウォータマークの内容に応じて暗号化コンテンツデータおよびライセンスが生成される。

上述したように、携帯電話機およびパーソナルコンピュータは、配信サーバから暗号化された暗号化コンテンツデータおよびライセンスを受信する。そして、携帯電話機およびパーソナルコンピュータのユーザは、受信した暗号化コンテンツデータおよびライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ移動または複製することもある。この場合、ユーザは、暗号化コンテンツデータを他のユーザの携帯電話機またはパーソナルコンピュータへ移動／複製することは自由でるが、暗号化コンテンツデータを復号するライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ自由に移動することはできない。つまり、ライセンスを他のユーザの携帯電話機またはパーソナルコンピュータへ移動／複製したとき、暗号化コンテンツデータの著作権保護の観点から送信側と受信側との両方にライセンスを残すことはできない。そこで、ライセンスの移動／複製を行なったとき、送信側のライセンスを消去する。

しかし、従来のライセンスの移動／複製の方法では、他のユーザへのライセンスの移動／複製の途中で通信が切断されたとき、他のユーザへはライセンスが届かず、送信側でもライセンスが消去された状態となり、移動／複製の対象となったライセンスを用いて暗号化コンテンツデータを復号できないという問題が生じる。

発明の開示

それゆえに、この発明の目的は、ライセンス等の一意義的にのみ存在が許容される独自データを他のデータ記録装置へ移動する途中で通信が切断されたときも、移動の対象となった独自データを復元可能なデータ記録装置を提供することである。

この発明によれば、データ記録装置は、一義的にのみ存在することが許容される独自データを他のデータ記録装置へ移動するデータ記録装置であって、他のデータ記録装置への独自データの移動処理を特定するための第１の履歴情報を保持する履歴情報保持部と、独自データを保持する独自データ保持部と、制御部とを備え、制御部は、独自データの他のデータ記録装置への移動に対して独自データの外部への出力が不可能な状態に変更し、独自データの復元要求に応じて、他の

データ記録装置との通信状態を示す他のデータ記録装置に保持された通信情報と他のデータ記録装置に保持された移動処理を特定するための第２の履歴情報とを他のデータ記録装置から受信し、通信情報に基づいて他のデータ記録装置との通信状態を確認し、通信情報が移動の途中を示すとき第２の履歴情報が第１の履歴情報に一致するか否かを判定し、第２の履歴情報が第１の履歴情報に一致するとき独自データの外部への出力が可能な状態に復元する。

好ましくは、独自データ保持部は、独自データの一部または全てを外部へ出力可能か出力不可かを示す出力可否フラグをさらに保持し、制御部は、独自データの他のデータ記録装置への移動に対して出力可否フラグを出力不可に設定し、独自データの復元時、出力可否フラグを出力可能に設定する。

好ましくは、履歴情報保持部は、移動の対象となった独自データを外部へ出力不可能な状態でさらに保持し、制御部は、独自データの他のデータ記録装置への移動に対して移動の対象となった独自データを履歴情報保持部に与え、独自データ保持部から移動の対象となった独自データを消去し、独自データの復元時、履歴情報保持部に保持された独自データを独自データ保持部に書込む。

好ましくは、第１の履歴情報は、移動のための通信確立時に他のデータ記録装置で生成され、かつ、他のデータ記録装置から受信された第１のセッション鍵であり、第２の履歴情報は、移動のための通信確立時に他のデータ記録装置で生成され、かつ、他のデータ記録装置に保持された第１のセッション鍵と同じ第２のセッション鍵である。

好ましくは、電子署名により通信情報と第２の履歴情報との正当性を確認する署名確認手段をさらに備え、制御部は、さらに、通信情報と第２の履歴情報とに対する電子署名を通信情報および第２の履歴情報とともに他のデータ記録装置から受信し、署名確認手段によって通信情報と第２の履歴情報の正当性が確認されたとき、通信状態を確認し、かつ、第１の履歴情報と第２の履歴情報との一致を確認する。

好ましくは、他のデータ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成部と、セッション鍵生成部が生成したセッション鍵によって暗号化されたデータを復号する復号部とをさらに備え、独自データの復元

時、セッション鍵生成部は、独自データの復元のための通信を特定する第３のセッション鍵を生成し、制御部は、第３のセッション鍵を他のデータ記録装置へ送信し、第３のセッション鍵によって暗号化された第２の履歴情報を他のデータ記録装置から受信する。

好ましくは、他のデータ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成部と、セッション鍵生成部が生成したセッション鍵によって暗号化されたデータを復号する復号部とをさらに備え、独自データの復元時、セッション鍵生成部は、独自データの復元のための通信を特定する第３のセッション鍵を生成し、制御部は、第３のセッション鍵を他のデータ記録装置へ送信し、第３のセッション鍵によって暗号化された第２の履歴情報と、第３のセッション鍵によって暗号化された電子署名のデータとを他のデータ記録装置から受信する。

好ましくは、履歴情報保持部は、移動の対象となった独自データに含まれる第１のデータ特定情報を第１の履歴情報とともに保持し、制御部は、さらに、他のデータ記録装置から受信する移動の対象となった第２のデータ特定情報が第１のデータ特定情報に一致するか否かを判定し、第２のデータ特定情報が第１のデータ特定情報に一致するとき、通信情報を確認し、かつ、第１の履歴情報と第２の履歴情報との一致を確認する。

好ましくは、電子署名により通信情報と第２の履歴情報と第２のデータ特定情報との正当性を確認する署名確認手段をさらに備え、制御部は、さらに、通信情報と第２の履歴情報と第２のデータ特定情報とに対する電子署名を、通信情報と第２の履歴情報と第２のデータ特定情報とともに受信し、署名確認手段によって通信情報と第２の履歴情報と第２のデータ特定情報の正当性が確認されたとき、第２のデータ特定情報と第１のデータ特定情報との一致を確認し、かつ、通信情報を確認し、第１の履歴情報と第２の履歴情報との一致を確認する。

好ましくは、他のデータ記録装置または他のデータ記録装置と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報を保持する通信情報保持部と、他のデータ記録装置またはもう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴

情報保持部とをさらに備え、制御部は、独自データの移動処理において移動対象となる独自データを他のデータ記録装置またはもう１つの他のデータ記録装置から受信するとき、第３の履歴情報をもう１つの履歴情報保持部に記録し、外部からの履歴情報の出力要求に応じて通信情報と第３の履歴情報とを出力する。

好ましくは、他のデータ記録装置またはもう１つの他のデータ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成部をさらに備え、セッション鍵生成部は、独自データの移動処理において移動対象となる独自データを他のデータ記録装置またはもう１つの他のデータ記録装置から受信するための通信を特定する第４のセッション鍵を生成し、制御部は、移動対象となる独自データを他のデータ記録装置またはもう１つのデータ記録装置から受信する通信の確立時、第４のセッション鍵を他のデータ記録装置またはもう１つのデータ記録装置へ送信するとともに第４のセッション鍵を第３の履歴情報としてもう１つの履歴情報保持部に格納し、外部からの履歴情報の出力要求に応じてもう１つの通信情報および第３の履歴情報を出力する。

好ましくは、もう１つの通信情報と第３の履歴情報とに対する電子署名を生成する電子署名生成部をさらに備え、制御部は、外部からの履歴情報の出力要求に応じて、もう１つの通信情報と第３の履歴情報と電子署名とを出力する。

好ましくは、他のデータ記録装置またはもう１つの他のデータ記録装置から入力された第５のセッション鍵によって暗号化する暗号処理部をさらに備え、制御部は、他のデータ記録装置またはもう１つの他のデータ記録装置から独自データを受信する通信の確立時、第４のセッション鍵を他のデータ記録装置またはもう１つの他のデータ記録装置に出力するとともに第４のセッション鍵を第３の履歴情報としてもう１つの履歴情報保持部に格納し、外部からの履歴情報の出力要求に応じてもう１つの通信情報と暗号処理部において第５のセッション鍵によって暗号化された第３の履歴情報とを出力する。

好ましくは、他のデータ記録装置またはもう１つの他のデータ記録装置から入力された第５のセッション鍵によってデータを暗号化する暗号処理部と、通信情報と暗号処理部において外部から入力された第３のセッション鍵によって暗号化された第３の履歴情報とに対する電子署名を生成する電子署名生成部とをさらに

備え、暗号処理部は、第５のセッション鍵によって第３の履歴情報と電子署名とを暗号化し、制御部は、他のデータ記録装置またはもう１つの他のデータ記録装置から独自データを受信する通信の確立時、第４のセッション鍵を他のデータ記録装置またはもう１つの他のデータ記録装置に出力するとともに第４のセッション鍵を第３の履歴情報としてもう１つの履歴情報保持部に格納し、外部からの履歴情報の出力要求に応じて、通信情報と第５のセッション鍵によって暗号化された第３の履歴情報と第５のセッション鍵によって暗号化された電子署名とを出力する。

好ましくは、制御部は、他のデータ記録装置またはもう１つの他のデータ記録装置からの移動の対象となる独自データを特定する第３のデータ特定情報を通信情報保持部に記録し、第３のデータ特定情報の出力要求に応じて、通信情報保持部から第３のデータ特定情報を読出して通信情報および第３の履歴情報とともに出力する。

好ましくは、独自データは、暗号化コンテンツデータを復号するためのライセンスである。

したがって、この発明によれば、他のデータ記録装置へ一義的にのみ存在することが許容される独自データを移動させている途中で通信が切断されても、移動の対象となった独自データを復元することができる。

図面の簡単な説明

図１は、データ配信システムを概念的に説明する概略図である。

図２は、他のデータ配信システムを概念的に説明する概略図である。

図３は、図１および図２に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

図４は、図１および図２に示すデータ配信システムにおける通信のためのデータ、情報等の特性を示す図である。

図５は、図１および図２に示すデータ配信システムにおける配信サーバの構成を示す概略ブロック図である。

図６は、図１および図２に示すデータ配信システムにおけるパーソナルコンピ

ュータの構成を示す概略ブロック図である。

図７は、図２に示すデータ配信システムにおける再生端末の構成を示す概略ブロック図である。

図８は、図１および図２に示すデータ配信システムにおけるメモリカードの構成を示す概略ブロック図である。

図９は、図１および図２に示すデータ配信システムにおける配信動作を説明するための第１のフローチャートである。

図１０は、図１および図２に示すデータ配信システムにおける配信動作を説明するための第２のフローチャートである。

図１１は、パーソナルコンピュータのハードディスクにおけるコンテンツリストファイルの構成を示す図である。

図１２は、メモリカードにおける再生リストファイルの構成を示す図である。

図１３は、メモリカード間の移動動作の概念を説明するための概略ブロック図である。

図１４は、図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動／複製動作を説明するための第１のフローチャートである。

図１５は、図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動／複製動作を説明するための第２のフローチャートである。

図１６は、図１および図２に示すデータ配信システムにおける暗号化コンテンツデータのライセンスの移動／複製動作を説明するための第３のフローチャートである。

図１７は、メモリカードのログ領域を説明するための概略ブロック図である。

図１８は、ライセンスの復元動作を説明するための第１のフローチャートである。

図１９は、ライセンスの復元動作を説明するための第２のフローチャートである。

図２０は、携帯電話機または再生端末における再生動作を説明するためのフロ

ーチャートである。

発明を実施するための最良の形態

本発明の実施の形態について図面を参照しながら詳細に説明する。なお、図中同一または相当部分には同一符号を付してその説明は繰返さない。

図１は、本発明によるデータ記録装置が暗号化コンテンツデータおよび暗号化コンテンツデータを復号するためのライセンスを取得するデータ配信システムの全体構成を概念的に説明するための概略図である。

なお、以下では携帯電話網を介して音楽データをユーザの携帯電話機に装着されたメモリカード１１０に、またはインターネットを介して音楽データを各パーソナルコンピュータに配信するデータ配信システムの構成を例にとって説明するが、以下の説明で明らかとなるように、本発明はこのような場合に限定されることなく、他の著作物としてのコンテンツデータ、たとえば画像データ、動画像データ等を配信する場合においても適用することが可能なものである。

図１を参照して、配信キャリア２０は、自己の携帯電話網を通じて得た、ユーザからの配信要求（配信リクエスト）を配信サーバ１０に中継する。音楽データを管理する配信サーバ１０は、データ配信を求めてアクセスして来た携帯電話ユーザの携帯電話機１００に装着されたメモリカード１１０が正当な認証データを持つか否か、すなわち、正規のメモリカードであるか否かの認証処理を行なう。そして、配信サーバ１０は、正当なメモリカードに対して著作権を保護するために所定の暗号方式により音楽データ（以下コンテンツデータとも呼ぶ）を暗号化した上で、データを配信するための配信キャリア２０である携帯電話会社に、このような暗号化コンテンツデータおよび暗号化コンテンツデータを再生するために必要な情報として暗号化コンテンツデータを復号するためのライセンス鍵を含むライセンスを与える。

配信キャリア２０は、自己の携帯電話網を通じて配信要求を送信した携帯電話機１００に装着されたメモリカード１１０に対して、携帯電話網および携帯電話機１００を介して暗号化コンテンツデータとライセンスとを配信する。

図１においては、たとえば携帯電話ユーザの携帯電話機１００には、着脱可能

なメモリカード１１０が装着される構成となっている。メモリカード１１０は、携帯電話機１００により受信された暗号化コンテンツデータを受取り、著作権を保護するために行なわれた暗号化を復号した上で、携帯電話機１００中の音楽再生回路（図示せず）に与える。

さらに、たとえば携帯電話ユーザは、携帯電話機１００に接続したヘッドホーン１３０等を介してこのようなコンテンツデータを「再生」して、聴取することが可能である。

このような構成とすることで、まず、メモリカード１１０を利用しないと、配信サーバ１０からコンテンツデータの配信を受けて、音楽を再生することが困難な構成となる。

しかも、配信キャリア２０において、たとえば１曲分のコンテンツデータを配信するたびにその度数を計数しておくことで、携帯電話ユーザがコンテンツデータを受信（ダウンロード）するたびに発生する著作権料を、配信キャリア２０が携帯電話機の通話料とともに徴収することとすれば、著作権者が著作権料を確保することが容易となる。

また、図１においては、配信サーバ１０は、インターネット網３０を通じて得た、パーソナルコンピュータ５０のユーザからの配信要求を受信する。そうすると、配信サーバ１０は、データ配信を求めてアクセスして来たパーソナルコンピュータ５０が正当な認証データを持つライセンス専用メモリカード（図示せず）を利用してアクセスしているか否か、すなわち、正規のライセンス専用メモリカードであるか否かの認証処理を行なう。そして、配信サーバ１０は、正当なライセンス専用メモリカードを備えたパーソナルコンピュータに対して、著作権を保護するために所定の暗号方式により音楽データを暗号化した暗号化コンテンツデータおよびその復号鍵であるライセンス鍵を含むライセンスをインターネット網３０を介して送信する。パーソナルコンピュータ５０のライセンス専用メモリカードはライセンスを格納する。

パーソナルコンピュータ５０は、メモリカード１１０のライセンス管理に関わる機能と同一機能を備えたライセンス専用メモリカード（ハードウェア）を備えることで、携帯電話機１００およびメモリカード１１０を用いて受信したのと同

じ配信を受けることができる。

さらに、パーソナルコンピュータ５０は、専用ケーブル６５によって携帯電話機１００と接続され、暗号化コンテンツデータおよびライセンスを携帯電話機１００に装着されたメモリカード１１０へ送信することが可能である。

したがって、図１に示すデータ配信システムにおいては、携帯電話機１００に装着されたメモリカード１１０は、携帯電話網を介して配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信して格納するとともに、パーソナルコンピュータ５０がインターネット網３０を介して配信サーバ１０から取得した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ５０から受けて格納することができる。

さらに、携帯電話機１００に装着されたメモリカード１１０は、携帯電話網を介して配信サーバ１０から受信した暗号化コンテンツデータおよびライセンスをパーソナルコンピュータ５０に待避することが可能となる。

図２は、携帯電話網を介して配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信する機能を有しない再生端末１０２を用いた場合のデータ配信システムを示したものである。図２に示すデータ配信システムにおいては、再生端末１０２に装着されたメモリカード１１０は、パーソナルコンピュータ５０が配信サーバ１０から取得した暗号化コンテンツデータおよびライセンスを受けて格納する。このように、パーソナルコンピュータ５０が暗号化コンテンツデータおよびライセンスを取得することによって通信機能のない再生端末１０２のユーザも暗号化コンテンツデータを受信することができるようになる。

図１および図２に示したような構成においては、暗号化して配信されるコンテンツデータを携帯電話機またはパーソナルコンピュータのユーザ側で再生可能とするためにシステム上必要とされるのは、第１には、通信におけるライセンスを配信するための方式であり、さらに第２には、コンテンツデータを暗号化する方式そのものであり、さらに、第３には、このようなコンテンツデータの無断コピーを防止するための著作権保護を実現する構成である。

本発明の実施の形態においては、特に、配信、および再生の各処理の発生時において、これらのライセンス鍵の出力先に対する認証およびチェック機能を充実

させ、非認証の記録装置（メモリカードおよびライセンス専用メモリカードなど）および再生端末（コンテンツ再生回路を備える携帯電話機やパーソナルコンピュータなど）に対するコンテンツデータの出力を防止することによってライセンス鍵の流出を防ぎ、著作権の保護を強化する構成を説明する。

なお、以下の説明においては、配信サーバ１０から、各携帯電話機、各パーソナルコンピュータ等に暗号化コンテンツデータまたはそのライセンスを伝送する処理を「配信」と称することとする。

図３は、図１および図２に示したデータ配信システムにおいて、使用される通信のためのデータ、情報等の特性を説明する図である。

まず、配信サーバ１０より配信されるデータについて説明する。Ｄｃは、音楽データ等のコンテンツデータである。コンテンツデータＤｃは、ライセンス鍵Ｋｃで復号可能な暗号化が施される。ライセンス鍵Ｋｃによって復号可能な暗号化が施された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃがこの形式で配信サーバ１０より携帯電話機１００またはパーソナルコンピュータ５０のユーザに配布される。

なお、以下においては、｛Ｙ｝Ｘという表記は、データＹを、復号鍵Ｘにより復号可能な暗号化を施したことを示すものとする。

さらに、配信サーバ１０からは、暗号化コンテンツデータとともに、コンテンツデータに関する著作権あるいはサーバアクセス関連等の平文情報としての付加情報Ｄｃ－ｉｎｆが配布される。また、ライセンスとしては、ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ等が存在する。ライセンスＩＤは、配信サーバ１０からのライセンスの配信を管理し、ライセンスを識別するためのコードであり、コンテンツＩＤは、コンテンツデータＤｃおよびライセンス鍵Ｋｃを識別するためのコードである。アクセス制御情報ＡＣｍは、記録装置（メモリカード、またはライセンス専用メモリカード）におけるライセンスのアクセスに対する制限に関する情報である。また、再生制御情報ＡＣｐは、コンテンツ再生回路における再生に関する制御情報である。具体的には、アクセス制御情報ＡＣｍは、メモリカード、およびライセンス専用メモリカードからのライセンスまたはライセンス鍵を外部に出力するに当っての制御情報であり、再生可能回数（再生のためにライセンス鍵を出

力する数）、ライセンスの移動・複製に関する制限情報などがある。再生制御情報ＡＣｐは、再生するためにコンテンツ再生回路がライセンス鍵を受取った後に、再生を制限する情報であり、再生期限、再生速度変更制限、および再生範囲指定（部分ライセンス）などがある。

以後、ライセンスＩＤと、コンテンツＩＤと、ライセンス鍵Ｋｃと、アクセス制御情報ＡＣｍと、再生制御情報ＡＣｐとを併せて、ライセンスと総称することとする。

また、以降では、簡単化のためアクセス制御情報ＡＣｍは再生回数の制限を行なう制御情報である再生回数（０：再生不可、１～２５４：再生可能回数、２５５：制限無し）、ライセンスの移動および複製を制限する移動・複製フラグ（０：移動複製禁止、１：移動のみ可、２：移動複製可）の２項目とし、再生制御情報ＡＣｐは再生可能な期限を規定する制御情報である再生期限（ＵＴＣｔｉｍｅコード）のみを制限するものとする。

本発明の実施の形態においては、送信元の記録装置（メモリカード、またはライセンス専用メモリカード）から受信先の記録装置へのライセンスの移動／複製において、送信元の記録装置に保持されたライセンスの有効・無効を示す有効フラグの運用を行なう。この有効フラグが有効であるとき、ライセンスをメモリカードから外部へ出すことが可能であることを意味し、有効フラグが無効であるとき、ライセンスをメモリカードから外部へ出すことができないことを意味する。

図４は、図１および図２に示すデータ配信システムにおいて使用される認証のためのデータ、情報等の特性を説明する図である。

データ再生端末内のコンテンツ再生回路、メモリカード、およびライセンス専用メモリカードには固有の公開暗号鍵ＫＰｐｙおよびＫＰｍｗがそれぞれ設けられる。公開暗号鍵ＫＰｐｙは、コンテンツ再生回路に固有の秘密復号鍵Ｋｐｙによって復号可能である。また、公開暗号鍵ＫＰｍｗは、メモリカード、およびライセンス専用メモリカードに固有の秘密復号鍵Ｋｍｗによって復号可能である。これら公開暗号鍵および秘密復号鍵は、メモリカード、およびライセンス専用メモリカードの種類ごとに異なる値を持つ。これらの公開暗号鍵および秘密復号鍵を総称してクラス鍵と称し、これらの公開暗号鍵をクラス公開暗号鍵、秘密復号

鍵をクラス秘密復号鍵、クラス鍵を共有する単位をクラスと称する。クラスは、製造会社や製品の種類、製造時のロット等によって異なる。

また、コンテンツ再生回路のクラス証明書としてＣｐｙが設けられ、メモリカード、およびライセンス専用メモリカードのクラス証明書としてＣｍｗが設けられる。これらのクラス証明書は、コンテンツ再生回路、メモリカード、およびライセンス専用メモリカードのクラスごとに異なる情報を有する。

コンテンツ再生回路のクラス公開暗号鍵およびクラス証明書は、認証データ｛ＫＰｐｙ／／Ｃｐｙ｝ＫＰａの形式で出荷時にデータ再生回路に記録される。また、メモリカード、およびライセンス専用メモリカードのクラス公開暗号鍵およびクラス証明書は認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａの形式で出荷時にメモリカード、およびライセンス専用メモリカードにそれぞれ記録される。後ほど詳細に説明するが、ＫＰａは配信システム全体で共通の公開認証鍵である。

また、メモリカード１１０、およびライセンス専用メモリカード内のデータ処理を管理するための鍵として、メモリカード１１０、およびライセンス専用メモリカードという媒体ごとに設定される公開暗号鍵ＫＰｍｃｘと、公開暗号鍵ＫＰｍｃｘで暗号化されたデータを復号することが可能なそれぞれに固有の秘密復号鍵Ｋｍｃｘが存在する。これらのメモリカードおよびライセンス専用メモリカードごとに設定される公開暗号鍵および秘密復号鍵を総称して個別鍵と称し、公開暗号鍵ＫＰｍｃｘを個別公開暗号鍵、秘密復号鍵Ｋｍｃｘを個別秘密復号鍵と称する。

ライセンスの配信、移動、複製および再生が行なわれるごとに配信サーバ１０、携帯電話機１００、メモリカード１１０、およびライセンス専用メモリカードにおいて生成される共通鍵Ｋｓ１～Ｋｓ３が用いられる。

ここで、共通鍵Ｋｓ１～Ｋｓ３は、配信サーバ、コンテンツ再生回路もしくはメモリカードもしくはライセンス専用メモリカード間の通信の単位あるいはアクセスの単位である「セッション」ごとに発生する固有の共通鍵であり、以下においてはこれらの共通鍵Ｋｓ１～Ｋｓ３を「セッションキー」とも呼ぶこととする。

これらのセッションキーＫｓ１～Ｋｓ３は、各セッションごとに固有の値を有

することにより、配信サーバ、コンテンツ再生回路、メモリカード、およびライセンス専用メモリカードによって管理される。具体的には、セッションキーＫｓ１は、配信サーバによって配信セッションごとに発生される。セッションキーＫｓ２は、メモリカード、およびライセンス専用メモリカードによって配信セッションおよび再生セッションごとに発生され、セッションキーＫｓ３は、コンテンツ再生回路において再生セッションごとに発生される。各セッションにおいて、これらのセッションキーを授受し、他の機器で生成されたセッションキーを受けて、このセッションキーによる暗号化を実行した上でライセンス鍵等の送信を行なうことによって、セッションにおけるセキュリティ強度を向上させることができる。

図５は、図１および図２に示した配信サーバ１０の構成を示す概略ブロック図である。

配信サーバ１０は、コンテンツデータを所定の方式に従って暗号化したデータやコンテンツＩＤ等の配信情報を保持するための情報データベース３０４と、携帯電話機やパーソナルコンピュータの各ユーザごとにコンテンツデータへのアクセスの開始に従った課金情報を保持するための課金データベース３０２と、情報データベース３０４に保持されたコンテンツデータのメニューを保持するメニューデータベース３０７と、ライセンスの配信ごとに生成され、かつ、ライセンスを特定するライセンスＩＤ等の配信に関するログを保持する配信記録データベース３０８と、情報データベース３０４、課金データベース３０２、メニューデータベース３０７、および配信記録データベース３０８からのデータをバスＢＳ１を介して受取り、所定の処理を行なうためのデータ処理部３１０と、通信網を介して、配信キャリア２０とデータ処理部３１０との間でデータ授受を行なうための通信装置３５０とを備える。

データ処理部３１０は、バスＢＳ１上のデータに応じて、データ処理部３１０の動作を制御するための配信制御部３１５と、配信制御部３１５によって制御され、配信セッション時にセッションキーＫｓ１を発生するためのセッションキー発生部３１６と、メモリカード、およびライセンス専用メモリカードから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを復号するための

公開認証鍵ＫＰａを保持する認証鍵保持部３１３と、メモリカード、およびライセンス専用メモリカードから送られてきた認証のための認証データ｛ＫＰｍｗ／／Ｃｍｗ｝ＫＰａを通信装置３５０およびバスＢＳ１を介して受けて、認証鍵保持部３１３からの公開認証鍵ＫＰａによって復号処理を行なう復号処理部３１２と、配信セッションごとに、セッション鍵Ｋｓ１を発生するセッションキー発生部３１６、セッションキー発生部３１６より生成されたセッションキーＫｓ１を復号処理部３１２によって得られたクラス公開暗号鍵ＫＰｍｗを用いて暗号化して、バスＢＳ１に出力するための暗号処理部３１８と、セッションキーＫｓ１によって暗号化された上で送信されたデータをバスＢＳ１より受けて、セッションキーＫｓ１により復号処理を行なう復号処理部３２０とを含む。

データ処理部３１０は、さらに、配信制御部３１５から与えられるライセンス鍵Ｋｃおよびアクセス制御情報ＡＣｍを、復号処理部３２０によって得られたメモリカード、およびライセンス専用メモリカードごとに個別な公開暗号鍵ＫＰｍｃｘによって暗号化するための暗号処理部３２６と、暗号処理部３２６の出力を、復号処理部３２０から与えられるセッションキーＫｓ２によってさらに暗号化してバスＢＳ１に出力するための暗号処理部３２８とを含む。

配信サーバ１０の配信セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図６は、図１および図２に示したパーソナルコンピュータ５０の構成を説明するための概略ブロック図である。パーソナルコンピュータ５０は、パーソナルコンピュータ５０の各部のデータ授受を行なうためのバスＢＳ２と、パーソナルコンピュータ５０内を制御すると共に、各種のプログラムを実行するためのコントローラ（ＣＰＵ）５１０と、バスＢＳ２に接続され、プログラムやデータを記録し、蓄積しておくための大容量記録装置であるハードディスク（ＨＤＤ）５３０およびＣＤ－ＲＯＭドライブ５４０と、ユーザからの指示を入力するためのキーボード５６０と、各種の情報を視覚的にユーザに与えるためのディスプレイ５７０とを含む。

パーソナルコンピュータ５０は、さらに、暗号化コンテンツデータおよびライセンスを携帯電話機１００等へ通信する際にコントローラ５１０と端子５８０と

の間でデータの授受を制御するためのＵＳＢ（Ｕｎｉｖｅｒｓａｌ　Ｓｅｒｉａｌ　Ｂｕｓ）インタフェース５５０と、専用ケーブル６５またはＵＳＢケーブル７５を接続するための端子５８０と、インターネット網３０を介して配信サーバ１０と通信する際にコントローラ５１０と端子５８５との間でデータの授受を制御するためのモデム５５５と、インターネット網３０と接続するための端子５８５とを含む。

コントローラ５１０は、インターネット網３０を介してライセンス専用メモリカード５２０に暗号化コンテンツデータ等を配信サーバ１０から受信するために、配信サーバ１０との間でデータの授受を制御する。さらに、パーソナルコンピュータ５０は、配信サーバ１０からの暗号化コンテンツデータおよびライセンスの受信を行なう際に配信サーバ１０との間で各種の鍵のやり取りを行ない、配信された暗号化コンテンツデータを再生するためのライセンスをハード的に管理するライセンス専用メモリカード５２０と、バスＢＳ２とライセンス専用メモリカード５２０との間でデータの授受を行なうメモリカードインタフェース５２５とを含む。

ライセンス専用メモリカード５２０は、暗号化コンテンツデータおよびライセンスを配信サーバ１０から受信する際のデータの授受をハード的に行ない、受信したライセンスをハード的に管理する。

このように、パーソナルコンピュータ５０は、配信サーバ１０からインターネット網３０を介して暗号化コンテンツデータおよびライセンスを受信したり、メモリカード１１０から待避されたライセンスを格納するためのライセンス専用メモリカード５２０を内蔵するものである。

図７は、図２に示した再生端末１０２の構成を説明するための概略ブロック図である。

再生端末１０２は、再生端末１０２の各部のデータ授受を行なうためのバスＢＳ３と、バスＢＳ３を介して再生端末１０２の動作を制御するためのコントローラ１１０６と、外部からの指示を再生端末１０２に与えるための操作パネル１１０８と、コントローラ１１０６等から出力される情報をユーザに視覚情報として与えるための表示パネル１１１０とを含む。

再生端末１０２は、さらに、配信サーバ１０からのコンテンツデータ（音楽データ）を記憶し、かつ、復号処理を行なうための着脱可能なメモリカード１１０と、メモリカード１１０とバスＢＳ３との間のデータの授受を制御するためのメモリカードインタフェース１２００と、パーソナルコンピュータ５０から暗号化コンテンツデータおよびライセンスを受信する際にバスＢＳ３と端子１１１４との間のデータ授受を制御するためのＵＳＢインタフェース１１１２と、ＵＳＢケーブル７５を接続するための端子１１１４とを含む。

再生端末１０２は、さらに、クラス公開暗号鍵ＫＰｐ１およびクラス証明書Ｃｐ１を公開認証鍵ＫＰａで復号することでその正当性を認証できる状態に暗号化した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを保持する認証データ保持部１５００を含む。ここで、再生端末１０２のクラスｙは、ｙ＝１であるとする。

再生端末１０２は、さらに、クラス固有の復号鍵であるＫｐ１を保持するＫｐ保持部１５０２と、バスＢＳ３から受けたデータを復号鍵Ｋｐ１によって復号し、メモリカード１１０によって発生されたセッションキーＫｓ２を得る復号処理部１５０４とを含む。

再生端末１０２は、さらに、メモリカード１１０に記憶されたコンテンツデータの再生を行なう再生セッションにおいてメモリカード１１０との間でバスＢＳ３上においてやり取りされるデータを暗号化するためのセッションキーＫｓ３を乱数等により発生するセッションキー発生部１５０８と、暗号化コンテンツデータの再生セッションにおいてメモリカード１１０からライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受取る際に、セッションキー発生部１５０８により発生されたセッションキーＫｓ３を復号処理部１５０４によって得られたセッションキーＫｓ２によって暗号化し、バスＢＳ３に出力する暗号処理部１５０６とを含む。

再生端末１０２は、さらに、バスＢＳ３上のデータをセッションキーＫｓ３によって復号して、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを出力する復号処理部１５１０と、バスＢＳ３より暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを受けて、復号処理部１５１０からのライセンス鍵Ｋｃによって暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号してコンテンツデータＤｃを音楽再生部１５１８へ出力する復号処理部１５１６とを含む。

再生端末１０２は、さらに、復号処理部１５１６からの出力を受けてコンテンツデータを再生するための音楽再生部１５１８と、音楽再生部１５１８の出力をディジタル信号からアナログ信号に変換するＤＡ変換器１５１９と、ＤＡ変換器１５１９の出力をヘッドホーンなどの外部出力装置（図示省略）へ出力するための端子１５３０とを含む。

なお、図７においては、点線で囲んだ領域は暗号化コンテンツデータを復号して音楽データを再生するコンテンツ再生回路１５５０を構成する。

一方、図１に示す携帯電話機１００は、携帯電話網を介して配信サーバ１０から暗号化コンテンツデータあるいはライセンスの配信を受信する機能を有するものである。したがって、図１に示す携帯電話機１００の構成は、図７に示す構成において、携帯電話網により無線伝送される信号を受信するためのアンテナと、アンテナからの信号を受けてベースバンド信号に変換し、あるいは携帯電話機からのデータを変調してアンテナに与えるための送受信部とマイクとスピーカと音声コーデック等の携帯電話機が本来備える機能を設けたものである。また、ＵＳＢインタフェース１１１２と端子１１１４とに代えて、それぞれ、専用ケーブルを接続するための専用インタフェースと専用端子とを備える。

携帯電話機１００、および再生端末１０２の各構成部分の各セッションにおける動作については、後ほどフローチャートを使用して詳細に説明する。

図８は、図１および図２に示すメモリカード１１０の構成を説明するための概略ブロック図である。

既に説明したように、メモリカードのクラス公開暗号鍵およびクラス秘密復号鍵として、ＫＰｍｗおよびＫｍｗが設けられ、メモリカードのクラス証明書Ｃｍｗが設けられるが、メモリカード１１０においては、自然数ｗ＝３で表わされるものとする。また、メモリカードを識別する自然数ｘはｘ＝４で表されるものとする。

したがって、メモリカード１１０は、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを保持する認証データ保持部１４００と、メモリカードごとに設定される固有の復号鍵である個別秘密復号鍵Ｋｍｃ４を保持するＫｍｃ保持部１４０２と、クラス秘密復号鍵Ｋｍ３を保持するＫｍ保持部１４２１と、個別秘密復号鍵Ｋｍｃ

４によって復号可能な公開暗号鍵ＫＰｍｃ４を保持するＫＰｍｃ保持部１４１６とを含む。

このように、メモリカードという記録装置の暗号鍵を設けることによって、以下の説明で明らかになるように、配信されたコンテンツデータや暗号化されたライセンス鍵の管理をメモリカード単位で実行することが可能になる。

メモリカード１１０は、さらに、メモリカードインタフェース１２００との間で信号を端子１４２６を介して授受するインタフェース１４２４と、インタフェース１４２４との間で信号をやり取りするバスＢＳ４と、バスＢＳ４にインタフェース１４２４から与えられるデータを、Ｋm保持部１４２１からのクラス秘密復号鍵Ｋｍ３により復号して、配信サーバ１０が配信セッションにおいて生成したセッションキーＫｓ1を接点Ｐａに出力する復号処理部１４２２と、ＫＰａ保持部１４１４から公開認証鍵ＫＰａを受けて、バスＢＳ４に与えられるデータから公開認証鍵ＫＰａによる復号処理を実行して復号結果と得られたクラス証明書をコントローラ１４２０に、得られたクラス公開鍵を暗号処理部１４１０に出力する復号処理部１４０８と、切換スイッチ１４４２によって選択的に与えられる鍵によって、切換スイッチ１４４６によって選択的に与えられるデータを暗号化してバスＢＳ４に出力する暗号処理部１４０６とを含む。

メモリカード１１０は、さらに、配信、および再生の各セッションにおいてセッションキーＫｓ２を発生するセッションキー発生部１４１８と、セッションキー発生部１４１８が出力したセッションキーＫｓ２を復号処理部１４０８によって得られるクラス公開暗号鍵ＫＰｐｙもしくはＫＰｍｗによって暗号化してバスＢＳ４に送出する暗号処理部１４１０と、バスＢＳ４よりセッションキーＫｓ２によって暗号化されたデータを受けてセッションキー発生部１４１８より得たセッションキーＫｓ２によって復号する復号処理部１４１２と、暗号化コンテンツデータの再生セッションにおいてメモリ１４１５から読出されたライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを、復号処理部１４１２で復号された他のメモリカードの個別公開暗号鍵ＫＰｍｃｘ（ｘ≠４）で暗号化する暗号処理部１４１７とを含む。

メモリカード１１０は、さらに、バスＢＳ４上のデータを個別公開暗号鍵ＫＰ

ｍｃ４と対をなすメモリカード１１０の個別秘密復号鍵Ｋｍｃ４によって復号するための復号処理部１４０４と、配信サーバ１０や他のメモリカードとの間の通信における履歴を格納するログと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを再生するためのライセンス（Ｋｃ，ＡＣｐ，ＡＣｍ，ライセンスＩＤ，コンテンツＩＤ）と、付加情報Ｄｃ－ｉｎｆと、暗号化コンテンツデータの再生リストと、ライセンスを管理するためのライセンス管理ファイルとをバスＢＳ４より受けて格納するためのメモリ１４１５とを含む。メモリ１４１５は、例えば半導体メモリによって構成される。また、メモリ１４１５は、ログ領域１４１５Ａと、ライセンス領域１４１５Ｂと、データ領域１４１５Ｃとから成る。ログ領域１４１５Ａは、ログを記録するための領域である。ログ領域１４１５Ａは、メモリカード１１０に対してライセンスが入力され、格納されるときに記録される受信ログと、メモリカード１１０が他のメモリカードに対してライセンスを出力するときに記録される送信ログとから成る。さらに、受信ログは、２つの状態（ＯＮ，ＯＦＦ）を持つ受信ｓｔａｔｅを含む。受信ログおよび送信ログの詳細については後述する。

ライセンス領域１４１５Ｂは、ライセンスを記録するための領域である。ライセンス領域１４１５Ｂは、ライセンス（ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、アクセス制限情報ＡＣｍ、ライセンスＩＤ、コンテンツＩＤ）と有効フラグとを記録するためにエントリと呼ばれるライセンス専用の記録単位でライセンスと有効フラグとを格納する。ライセンスに対してアクセスする場合には、ライセンスが格納されている、あるいは、ライセンスを記録したいエントリをエントリ番号によって指定する構成になっている。

データ領域１４１５Ｃは、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃ、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃの関連情報Ｄｃ－ｉｎｆ、ライセンスを管理するために必要な情報を暗号化コンテンツごとに記録するライセンス管理ファイル、メモリカードに記録された暗号化コンテンツデータやライセンスにアクセスするための基本的な情報を記録する再生リスト、およびライセンス領域１４１５Ｂのエントリを管理するためのエントリ情報を記録するための領域である。そして、データ領域１４１５Ｃは、外部から直接アクセスが可能である。ライセンス管理ファ

イルおよび再生リストの詳細については後述する。

メモリカード１１０は、さらに、バスＢＳ４を介して外部との間でデータ授受を行ない、バスＢＳ４との間でアクセス制御情報ＡＣｍ等を受けて、メモリカード１１０の動作を制御するためのコントローラ１４２０を含む。

なお、データ領域１４１５Ｃを除く全ての構成は、耐タンパモジュール領域に構成される。

また、図６に示すライセンス専用メモリカード５２０は、メモリカード１１０と同じ構成から成る。ただし、ライセンス専用メモリカード５２０は、メモリ１４１５内のデータ領域１４１５Ｃにエントリ管理情報のみを記録する。そして、ライセンス専用メモリカード５２０における自然数ｗは３以外の値を有し、ライセンス専用メモリカード５２０を識別するための自然数ｘは４以外の値を持つ。

以下、図１および図２に示すデータ配信システムにおける各セッションの動作について説明する。

［配信］

まず、図１に示すデータ配信システムにおいて、配信サーバ１０から携帯電話機１００のメモリカード１１０へ暗号化コンテンツデータおよびライセンスを配信する動作について説明する。

図９および図１０は、図１に示すデータ配信システムにおける暗号化コンテンツデータの購入時に発生する携帯電話機１００に装着されたメモリカード１１０へのライセンスの配信動作（以下、配信セッションともいう）を説明するための第１および第２のフローチャートである。

図９における処理以前に、携帯電話機１００のユーザは、配信サーバ１０に対して電話網を介して接続し、購入を希望するコンテンツに対するコンテンツＩＤを取得し、さらに、メモリカード１１０に対するエントリ管理情報を取得してライセンス領域１４１５Ｂ内の空きエントリを確認していることを前提としている。

図９を参照して、携帯電話機１００のユーザから操作パネル１１０８を介してコンテンツＩＤの指定による配信リクエストがなされる（ステップＳ１００）。そして、携帯電話機１００のユーザは、操作パネル１１０８を介して暗号化コン

テンツデータのライセンスを購入するための購入条件ＡＣを入力するように指示し、購入条件ＡＣが入力される（ステップＳ１０２）。つまり、選択した暗号化コンテンツデータを復号するライセンス鍵Ｋｃを購入するために、暗号化コンテンツデータのアクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐを設定して購入条件ＡＣが入力される。

暗号化コンテンツデータの購入条件ＡＣが入力されると、コントローラ１１０６は、バスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ認証データの出力指示を与える（ステップＳ１０４）。メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ１０６）。そして、コントローラ１４２０は、バスＢＳ４を介して認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを読出し、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４、インタフェース１４２４および端子１４２６を介して出力する（ステップＳ１０８）。

携帯電話機１００のコントローラ１１０６は、メモリカード１１０からの認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａに加えて、コンテンツＩＤ、ライセンス購入条件のデータＡＣ、および配信リクエストを配信サーバ１０に対して送信する（ステップＳ１１０）。

配信サーバ１０は、携帯電話機１００から配信リクエスト、コンテンツＩＤ、認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａ、およびライセンス購入条件のデータＡＣを受信し（ステップＳ１１２）、復号処理部３１２は、メモリカード１１０から出力された認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを公開認証鍵ＫＰａで復号する（ステップＳ１１４）。

配信制御部３１５は、復号処理部３１２における復号処理結果から、正規の機関でその正当性を証明するための暗号化を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ１１６）。正当な認証データであると判断された場合、配信制御部３１５は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ１１８）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ

３およびクラス証明書Ｃｍ３を受理しないで配信セッションを終了する（ステップＳ１６４）。

認証の結果、正当な認証データを持つメモリカードを装着した携帯電話機からのアクセスであることが確認されると、配信サーバ１０において、セッションキー発生部３１６は、配信のためのセッションキーＫｓ１を生成する（ステップＳ１１８）。セッションキーＫｓ１は、復号処理部３１２によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号処理部３１８によって暗号化される（ステップＳ１２０）。

配信制御部３１５は、ライセンスＩＤを生成し（ステップＳ１２２）、ライセンスＩＤおよび暗号化されたセッションキーＫｓ１は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３として、バスＢＳ１および通信装置３５０を介して携帯電話機１００へ送信される（ステップＳ１２４）。

携帯電話機１００が、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３を受信すると、コントローラ１１０６は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３をメモリカード１１０に入力する（ステップＳ１２６）。そうすると、メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、コントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ１｝Ｋｍ３を受理する（ステップＳ１２８）。そして、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のログ領域１４１５Ａに記録されている受信ログを初期化し、受理したライセンスＩＤをログ領域１４１５Ａに格納する（ステップＳ１３０）。このとき、受信ログ内の受信ｓｔａｔｅは、ＯＦＦに設定される。その後、コントローラ１４２０は、バスＢＳ４を介して暗号化データ｛Ｋｓ１｝Ｋｍ３を復号処理部１４２２へ与え、復号処理部１４２２は、Ｋｍ保持部１４２１に保持されるメモリカード１１０に固有なクラス秘密復号鍵Ｋｍ３によって復号処理することにより、セッションキーＫｓ１を復号し、セッションキーＫｓ１を受理する（ステップＳ１３２）。

コントローラ１４２０は、配信サーバ１０で生成されたセッションキーＫｓ１の受理を確認すると、セッションキー発生部１４１８に対してメモリカード１１０において配信動作時に生成されるセッションキーＫｓ２の生成を指示する。そ

して、セッションキー発生部１４１８は、セッションキーＫｓ２を生成する（ステップＳ１３４）。コントローラ１４２０は、生成されたセッション鍵Ｋｓ２をバスＢＳ４を介して受取り、その受取ったセッション鍵Ｋｓ２をメモリ１４１５のログ領域１４１５Ａに格納し、受信ｓｔａｔｅをＯＮにする（ステップＳ１３６）。

暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐａを介して復号処理部１４２２より与えられるセッションキーＫｓ１によって、切換スイッチ１４４６の接点を順次切換えることによって与えられるセッションキーＫｓ２、および個別公開暗号鍵ＫＰｍｃ４を１つのデータ列として暗号化して、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１をバスＢＳ４に出力する。バスＢＳ４に出力された暗号化データ｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１は、バスＢＳ４からインタフェース１４２４および端子１４２６を介して携帯電話機１００に出力され（ステップＳ１３８）、携帯電話機１００から配信サーバ１０に送信される（ステップＳ１４０）。

図１０を参照して、配信サーバ１０は、暗号化データ｛Ｋｓ２／／ＫＰｍｃ４｝Ｋｓ１を受信して、復号処理部３２０においてセッションキーＫｓ１による復号処理を実行し、メモリカード１１０で生成されたセッションキーＫｓ２、およびメモリカード１１０の個別公開暗号鍵ＫＰｍｃ４を受理する（ステップＳ１４２）。

配信制御部３１５は、ステップＳ１１２で取得したコンテンツＩＤに従ってライセンス鍵Ｋｃを情報データベース３０４から取得し（ステップＳ１４４）、ステップＳ１１２で取得したライセンス購入条件ＡＣに従って、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐを決定する（ステップＳ１４６）。

配信制御部３１５は、生成したライセンス、すなわち、ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、およびアクセス制御情報ＡＣｍを暗号処理部３２６に与える。暗号処理部３２６は、復号処理部３２０によって得られたメモリカード１１０の個別公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成する（ステップＳ１４８）。そして、暗号

処理部３２８は、暗号処理部３２６からの暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を、復号処理部３２０からのセッションキーＫｓ２によって暗号化し、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を出力する。配信制御部３１５は、バスＢＳ１および通信装置３５０を介して暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を携帯電話機１００へ送信する（ステップＳ１５０）。

携帯電話機１００は、送信された暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２を受信し、バスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０に入力する（ステップＳ１５２）。メモリカード１１０においては、端子１４２６およびインタフェース１４２４を介して、バスＢＳ４に与えられた受信データを復号処理部１４１２によって復号する。復号処理部１４１２は、セッションキー発生部１４１８から与えられたセッションキーＫｓ２を用いてバスＢＳ４の受信データを復号し、バスＢＳ４に出力する（ステップＳ１５４）。

この段階で、バスＢＳ４には、Ｋｍｃ保持部１４０２に保持される個別秘密復号鍵Ｋｍｃ４で復号可能な暗号化ライセンス｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４が出力される（ステップＳ１５４）。

コントローラ１４２０の指示によって、暗号化ライセンス｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、個別秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ１５６）。

携帯電話機１００のコントローラ１１０６は、メモリカード１１０のメモリ１４１５から読出したエントリ管理情報に基づいて、配信サーバ１０から受信したライセンスを格納するためのエントリ番号を決定し、その決定したエントリ番号をバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０へ入力する（ステップＳ１５８）。

そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ステップＳ１５６において取得したライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）を格納し、同一エントリにおける有効フラグを有効にする（ステップＳ１６０）。そして、コントローラ１４２０は、バスＢＳ４を介してメモリ１４１５のログ領域１４１５Ａの受信ログに記録された受信ｓｔａｔｅをＯＦＦする（ステップＳ１６１）。ライセンスの書込みが終了すると、コントローラ１１０６は、ステップＳ１５８においてメモリカード１１０へ入力したエントリが使用中であるようにエントリ管理情報を更新し、その更新したエントリ管理情報をメモリカード１１０へ入力する（ステップＳ１６２）。メモリカード１１０のコントローラ１４２０は、入力されたエントリ管理情報を用いてメモリ１４１５のデータ領域１４１５Ｃ内にエントリ管理情報を書換える（ステップＳ１６３）。そして、ライセンスの配信動作が終了する（ステップＳ１６４）。

ライセンスの配信セッションが終了した後、携帯電話機１００のコントローラ１１０６は、暗号化コンテンツデータの配信要求を配信サーバ１０へ送信し、配信サーバ１０は、暗号化コンテンツデータの配信要求を受信する。そして、配信サーバ１０の配信制御部３１５は、情報データベース３０４より、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを取得して、これらのデータをバスＢＳ１および通信装置３５０を介して携帯電話機１００へ送信する。

携帯電話機１００は、データ｛Ｄｃ｝Ｋｃ／／Ｄｃ－ｉｎｆを受信して、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを受理する。そうすると、コントローラ１１０６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃおよび付加情報Ｄｃ－ｉｎｆを１つのコンテンツファイルとしてバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０に入力する。また、コントローラ１１０６は、メモリカード１１０に格納されたライセンスのエントリ番号と、平文のライセンスＩＤと、コンテンツＩＤとを含み、かつ、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとに対するライセンス

管理ファイルを生成し、その生成したライセンス管理ファイルをバスＢＳ３およびメモリカードインタフェース１２００を介してメモリカード１１０に入力する。さらに、コントローラ１１０６は、メモリカード１１０のメモリ１４１５に記録されている再生リストに、受理したコンテンツの情報として、記録したコンテンツファイル及びライセンス管理ファイルの名称や付加情報Ｄｃ－ｉｎｆから抽出した暗号化コンテンツデータに関する情報（曲名、アーティスト名）等を追記し、全体の処理が終了する。

このようにして、携帯電話機１００に装着されたメモリカード１１０が正規の認証データを保持する機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上でコンテンツデータを配信することができ、不正なメモリカードへのコンテンツデータの配信を禁止することができる。

さらに、配信サーバおよびメモリカードでそれぞれ生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、データ配信システムのセキュリティを向上させることができる。

また、メモリカード１１０は、配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信する際に、配信サーバ１０との間でハード的にデータのやり取りを行ない、暗号化コンテンツデータを再生するためのライセンスをハード的に格納するため、そのセキュリティレベルは高い。

図６に示すライセンス専用メモリカード５２０へのライセンスの配信動作も図９および図１０に示すフローチャートに従って行なわれる。また、ライセンス専用メモリカード５２０への暗号化コンテンツデータの配信動作も上述したのと同じ動作によって行なわれる。すなわち、上記の説明において、携帯電話機１００をパーソナルコンピュータ５０に代え、メモリカード１１０をライセンス専用メモリカード５２０に代えれば良い。その他は、上述したのと同じである。

ライセンス専用メモリカード５２０への暗号化コンテンツデータおよびライセンスの配信においても暗号化コンテンツデータおよびライセンスをハード的に受

信し、かつ、格納するので、ライセンス専用メモリカード５２０への暗号化コンテンツデータおよびライセンスの配信は、メモリカード１１０への暗号化コンテンツデータおよびライセンスの配信と同じようにセキュリティレベルが高い。

図１１を参照して、パーソナルコンピュータ５０のライセンス専用メモリカード５２０によって受信された暗号化コンテンツデータおよびライセンスの管理について説明する。パーソナルコンピュータ５０のハードディスク５３０は、再生リスト１５０と、コンテンツファイル１５３１～１５３５と、ライセンス管理ファイル１５２１～１５２５とを含む。

再生リスト１５０は、所有するコンテンツの一覧形式のデータファイルであり、個々のコンテンツに対する情報（楽曲名、アーティスト名など）と、コンテンツファイルとライセンス管理ファイルとを示す情報（ファイル名）などが含まれている。個々のコンテンツに対する情報は受信時に付加情報Ｄｃ－ｉｎｆから必要な情報を取得して自動的に、あるいは、ユーザの指示によって記載される。また、コンテンツファイルのみ、またはライセンス管理ファイルのみの再生できないコンテンツについても一覧の中で管理することが可能である。

コンテンツファイル１５３１～１５３５は、ライセンス管理デバイス５２０によって受信された暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを記録するファイルであり、コンテンツごとに設けられる。

また、ライセンス管理ファイル１５２１～１５２５は、それぞれ、コンテンツファイル１５３１～１５３５に対応して記録されており、ライセンス専用メモリカード５２０に受信され、記録されているライセンスを管理するためのファイルである。これまでの説明でも明らかなように、ライセンスは通常参照することができないが、ライセンス鍵Ｋｃを除く他の情報は、ユーザが書き換えることさえできなければ著作権保護の点では問題ない。しかし、運用においてライセンス鍵Ｋｃと分離して管理することはセキュリティの低下につながるため好ましくない。そこで、ライセンスの配信を受ける場合に平文にて参照できるライセンスＩＤ、コンテンツＩＤや、ライセンス購入条件ＡＣから容易に判断できるアクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐにて制限されている事項の写しを平文にて記録する。さらに、ライセンス専用メモリカード５２０にライセンスが記録

された場合にエントリ番号を記録する。ライセンス専用メモリカード５２０のメモリ５２１５のライセンス領域５２５Ｂは、高いセキュリティレベルでライセンスを記録する耐タンパモジュールで構成された記録領域である。ライセンス（ライセンス鍵Ｋｃ、再生制御情報ＡＣｐ、アクセス制限情報ＡＣｍ、ライセンスＩＤ）を記録するためにM個のエントリを備えている。

ライセンス管理ファイル１５２１，１５２４，１５２２，１５２５は、それぞれ、エントリ番号０，１，２，３，を含む。これは、ライセンス専用メモリカード５２０によって受信され、ライセンス専用メモリカード５２０のメモリ５２１５のライセンス領域５２１５Ｂにおいて管理されるライセンス（ライセンスＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｍ）の管理領域を指定する番号である。

また、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを携帯電話機１００または再生端末１０２に装着されたメモリカード１１０へ移動させるとき、コンテンツファイル１５３１～１５３５を検索してコンテンツファイル１５３１を抽出すれば、暗号化コンテンツデータを再生するライセンスがどこで管理されているかが解かる。コンテンツファイル１５３１に対応するライセンス管理ファイル１５２１に含まれるエントリ番号は「０」であるので、コンテンツファイル１５３１に記録されたファイル名の暗号化コンテンツデータを再生するライセンスは、ライセンス専用メモリカード５２０のメモリ５２１５のライセンス領域５２１５Ｂのエントリ番号０によって指定された領域に記録されている。そうすると、ハードディスク５３０に記録された再生リストファイル１５０のライセンス管理ファイル１５２１からエントリ番号０を読出し、その読出したエントリ番号０をライセンス専用メモリカード５２０に入力することによって、メモリ５２１５のライセンス領域５２１５Ｂからライセンスを容易に取出し、メモリカード１１０へ移動できる。そして、ライセンスを移動した後は、メモリ５２１５のライセンス領域５２１５Ｂにおいて指定されたエントリ番号内の有効フラグは無効になり、それに対応してライセンス管理ファイル１５２３のように「ライセンス無」が記録される。

ライセンス管理ファイル１５２３は、「ライセンス無」を含む。これは、ライ

センス専用メモリカード５２０によって受信されたライセンスが、メモリカードや他のライセンス専用メモリカードへ移動された結果である。対応するコンテンツファイル１５３３はハードディスク５３０に記録されたままになっている。メモリカードや他のライセンス専用メモリカードからライセンスを再びライセンス専用メモリカード５２０へ移動、あるいは、配信サーバ１０から再び配信を受ける場合には、ライセンスについてのみ配信を受けることが可能である。また、エントリ管理情報１５５がライセンス専用メモリカード５２０のデータ領域５２１５Ｃに記録されている。エントリ管理情報１５５は、ライセンス専用メモリカード５２０のライセンス領域５２１５Ｂのエントリの使用状態を示す情報である。したがって、エントリ管理情報１５５を参照すれば、エントリの使用状態が解かる。

図１２は、メモリカード１１０のメモリ１４１５におけるライセンス領域１４１５Ｂとデータ領域１４１５Ｃとを示したものである。データ領域１４１５Ｃには、再生リストファイル１６０と、エントリ管理情報１６５と、コンテンツファイル１６１１～１６１ｎと、ライセンス管理ファイル１６２１～１６２ｎとが記録されている。コンテンツファイル１６１１～１６１ｎは、受信した暗号化コンテンツデータ｛Ｄｃ｝Ｋｃと付加情報Ｄｃ－ｉｎｆとを１つのファイルとして記録する。また、ライセンス管理ファイル１６２１～１６２ｎは、それぞれ、コンテンツファイル１６１１～１６１ｎに対応して記録されている。

メモリカード１１０は、配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信したとき、パーソナルコンピュータ５０から暗号化コンテンツデータおよびライセンスを「移動セッション」によって受信したとき、暗号化コンテンツデータおよびライセンスをメモリ１４１５に記録する。

したがって、パーソナルコンピュータ５０のライセンス専用メモリカード５２０によって受信され、かつ、移動セッションによってメモリカード１１０に送信されたセキュリティレベルの高い暗号化コンテンツデータのライセンスは、メモリ１４１５のライセンス領域１４１５Ｂのエントリ番号によって指定された領域に記録され、メモリ１４１５のデータ領域１４１５Ｃに記録された再生リストファイル１６０のライセンス管理ファイルを読出せば、エントリ番号を取得でき、

その取得したエントリ番号によって対応するライセンスをライセンス領域１４１５Ｂから読出すことができる。

また、ライセンス管理ファイル１６２２は、点線で示されているが、実際には記録されていないことを示す。コンテンツファイル１６１２は存在しているがライセンスが無く再生できないことを表しているが、これは、たとえば、再生端末が他の携帯電話機から暗号化コンテンツデータだけを受信した場合に相当する。

また、コンテンツファイル１６１３は、点線で示されているが、これは、たとえば、再生端末が配信サーバ１０から暗号化コンテンツデータおよびライセンスを受信し、その受信した暗号化コンテンツデータだけを他の携帯電話機へ送信した場合に相当し、ライセンスはメモリ１４１５に存在するが暗号化コンテンツデータが存在しないことを意味する。

［移動／複製］

上述したように、図１に示すデータ配信システムにおいて、携帯電話機１００に装着されたメモリカード１１０は、携帯電話網を介して配信サーバ１０からライセンスを受信して記録することができる。また、図１および図２に示すデータ配信システムにおいて、パーソナルコンピュータ５０に装着されたライセンス専用メモリカード５２０は、インターネット網３０を介して配信サーバ１０からライセンスを受信して記録することができる。

また、図１および図２のデータ配信システムにおけるメモリカード１１０またはライセンス専用メモリカード５２０は、記録されているライセンスを他のメモリカード（ライセンス専用メモリカードを含む）に安全に移動／複製させるための機能を備えており、記録されているライセンスを他のメモリカードに移動／複製することができる。当然のことながら、メモリカード１１０とライセンス専用メモリカード５２０との間においてもライセンスの移動／複製を行なうことができる。

したがって、図１および図２に示すデータ配信システムでは、パーソナルコンピュータ５０に装着されたライセンス専用メモリカード５２０に記録されたライセンスを携帯電話機１００または再生端末１０２に装着されたメモリカード１１０へ移動／複製させることができる。また、逆に、携帯電話機１００または再生

端末１０２に装着されたメモリカード１１０に記録されたライセンスをパーソナルコンピュータ５０に装着されたライセンス専用メモリカード５２０に移動／複製させることができる。その結果、ユーザの利便性の向上を図ることができる。

また、暗号化コンテンツデータは、自由にアクセス可能なパーソナルコンピュータ５０のハードディスク５３０またはメモリカード１１０のデータ領域１４１５Ｃに記録されているので自由に複製可能であるが、ライセンスの移動／複製が伴わなければ再生することができない。

そこで、メモリカード１１０またはライセンス専用メモリカード５２０に記録されているライセンスを他のメモリカードに移動／複製するときの動作について説明する。

この場合、図８に示す構成を有する２つのメモリカード間でライセンスの移動／複製が行なわれ、パーソナルコンピュータ５０、携帯電話機１１０および再生端末１０２は、それぞれ、装着されたメモリカード（ライセンス専用メモリカードを含む）に対するデータの入出力処理と通信路を提供し、データの中継処理を行なうのみであるため説明を簡単にするために図１３に示すような系を考える。

図１３に示す系は、コントローラ４０と、メモリカードを制御するインタフェース６０と、２枚のメモリカード１１０，１２０によって構成される。図１に示すデータ配信システムを想定するとパーソナルコンピュータ５０に装着されたライセンス専用メモリカード５２０から携帯電話機１００に装着されたメモリカード１１０に、または携帯電話機１００に装着されたメモリカード１１０からパーソナルコンピュータ５０に装着されたライセンス専用メモリカード５２０に、ライセンスを移動／複製することを想定すると、メモリカード１２０はライセンス専用メモリカード５２０、インタフェース６０はパーソナルコンピュータ５０のメモリカードインタフェース５２５および携帯電話機１００のメモリカードインタフェース１２００に相当する。さらに、コントローラ４０は、パーソナルコンピュータ５０のコントローラ５１０および携帯電話機１００のコントローラ１１０６の機能を行ない、パーソナルコンピュータ５０と携帯電話機１００との間の通信に関する部分を省略したものである。また、図２に示すデータ配信システムを想定する場合には、携帯電話機１００を再生端末１０２に読替えればよい。

また、図１に示すデータ配信システムにおいて、携帯電話機１００が公衆網を介して他の携帯電話機に対してライセンスの移動／複製を行なうことも可能である。さらに、図１および図２に示すデータ配信システムにおける携帯電話機１００または再生端末１０２が端末間の独自の通信手段を備え、携帯電話機１００または再生端末１０２から他の携帯電話機または再生端末へライセンスの移動／複製を行なうことも可能である。この場合、メモリカード１２０は、他の携帯電話機または再生端末に装着されたメモリカードに相当する。インタフェース６０は、携帯電話機１００または再生端末１０２のメモリカードインタフェース１２００と通信相手である他の携帯電話機または再生端末のメモリカードインタフェースに相当する。コントローラ４０は、携帯電話機１００または再生端末１０２のコントローラ１１０６と通信相手である他の携帯電話機または再生端末のコントローラに相当する。そして、図１３においては、通信手段を用いた通信に関する部分を省略したものである。

さらに、図７に示した再生端末１０２は、メモリカードを１枚装着する構成であるが、２枚以上のメモリカードを装着するような構成にすることも可能である。この場合、コントローラ４０は、再生端末１０２のコントローラ１１０６に相当し、インタフェース６０は、２枚以上装着できるように変更したメモリカードインタフェース１２００に相当する。携帯電話機１００においても、２枚以上のメモリカードを装着可能な構成に変更することも可能である。その場合、再生端末１０２を携帯電話機１００に読替えればよい。

また、さらに、メモリカード１１０へのデータの書込みおよび読出しを行なうメモリカードライタやパーソナルコンピュータに装着されたメモリカードドライブ装置を用いてライセンスの移動／複製を行なう系を構成することも可能である。

図１４～図１６は、図１３におけるメモリカード１２０に記録されたライセンスをメモリカード１１０に移動／複製するためのフローチャートである。なお、図１４における処理以前に、コントローラ４０は、ユーザがライセンスの移動／複製を行なうコンテンツの指定およびライセンスの移動／複製リクエストを行なうための入力手段（図示せず）に接続され、ユーザによってなされたライセンス

の移動／複製を行なうコンテンツの指定、およびライセンスの移動／複製リクエストを受取る。そして、コントローラ４０は、送信側であるメモリカード１２０内の再生リストを参照してライセンスの移動／複製を行なうライセンス管理ファイルを取得していることを前提としている。また、送信側のメモリカード１２０および受信側のメモリカード１１０内に格納されている、それぞれのエントリ管理情報を取得していることを前提としている。さらに、受信側のメモリカード１２０に格納されたエントリ管理情報によって、受信側のメモリカード１１０のライセンス領域１４１５Ｂ内に空きのエントリを確認していることを前提としている。

図１４を参照して、移動／複製リクエストがユーザから指示されると（ステップＳ３００）、コントローラ４０は、メモリカード１１０へ認証データの送信要求をインタフェース６０を介してメモリカード１１０へ送信する（ステップＳ３０２）。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ３０４）。

メモリカード１１０のコントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４、インタフェース１４２４および端子１４２６を介してインタフェース６０へ出力する（ステップＳ３０６）。そして、コントローラ４０は、インタフェース６０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受取り、インタフェース６０を介してメモリカード１２０へメモリカード１１０の認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを送信する（ステップＳ３０８）。

そうすると、メモリカード１２０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４を介して復号処理部１４０８へ与える。そして、復号処理部１４０８は、ＫＰａ保持部１４１４からの公開認証鍵ＫＰａによって認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａの復号処理を実行する（ステップＳ３１０）。コントローラ１４２０

は、復号処理部５２０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードであって、メモリカード１１０から正規の機関でその正当性を証明するための暗号を施した認証データを受信したか否かを判断する認証処理を行なう（ステップＳ３１２）。正当な認証データであると判断された場合、コントローラ１４２０は、認証データから取得されたクラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ３１４）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ３７０）。

認証の結果、正当な認証データを持つメモリカードへのライセンスの移動／複製であることが確認されると、メモリカード１２０において、コントローラ１４２０は、セッションキー発生部１４１８を制御し、セッションキー発生部１４１８は、移動のためのセッションキーＫｓ２ａを生成する（ステップＳ３１４）。セッションキーＫｓ２ａは、復号処理部１４０８によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号処理部１４１０によって暗号化される。そして、メモリカード１２０のコントローラ１４２０は、バスＢＳ４を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を取得し、バスＢＳ４、インタフェース１４２４および端子１４２６を介してインタフェース６０に出力する（ステップＳ３１６）。

コントローラ４０は、インタフェース６０を介して暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を送信側から受理し（ステップＳ３１８）、送信側のメモリカード１２０のライセンス管理情報からライセンスＩＤを取得する（ステップＳ３２０）。そして、コントローラ４０は、取得したライセンスＩＤと、ステップＳ３１８において受理した暗号化データ｛Ｋｓ２ａ｝Ｋｍ３とを１つにデータにしてライセンスＩＤ／／｛Ｋｓ２ａ｝Ｋｍ３をインタフェース６０を介してメモリカード１１０へ入力する（ステップＳ３２２）。そうすると、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介してライセンスＩＤ／／｛Ｋｓ２ａ｝Ｋｍ３を受理する。そして、メモリカード１１０のコントローラ１４２０は、メモリ１４１５のログ領域１４１５Ａを

初期化し、受理したライセンスＩＤをログ領域１４１５Ａに格納する（ステップＳ３２６）。この受信ログの初期化によって暗号化コンテンツデータのライセンスの配信時に格納されたライセンスＩＤおよびセッションキーＫｓ２（図９のステップＳ１３０，Ｓ１３６）が消去され、受信ｓｔａｔｅがＯＦＦされる。その後、コントローラ１４２０は、暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を復号処理部１４２２へ与え、復号処理部１４２２は、Ｋｍ保持部１４２１からのクラス秘密復号鍵Ｋｍ３によって暗号化データ｛Ｋｓ２ａ｝Ｋｍ３を復号してセッションキーＫｓ２ａを受理する（ステップＳ３２８）。そして、セッションキー発生部１４１８は、セッションキーＫｓ２ｂを生成し（ステップＳ３３０）、コントローラ１４２０は、バスＢＳ４を介してセッションキーＫｓ２ｂを受取り、その受取ったセッションキーＫｓ２ｂをメモリ１４１５のログ領域１４１５Ａの受信ログに格納して受信ｓｔａｔｅをＯＮにする（ステップＳ３３２）。このセッションキーＫｓ２ｂの格納によってメモリカード１２０からメモリカード１１０へのライセンスの移動／複製処理を特定するための履歴情報が受信ログに記録されたことになる。

そうすると、メモリカード１１０の暗号処理部１４０６は、切換スイッチ１４４６の端子を順次切換えることによって、セッションキー発生部１４１８で発生されたセッションキーＫｓ２ｂ、および個別公開暗号鍵ＫＰｍｃ４を、復号処理部１４０４によって復号されたセッションキーＫｓ２ａによって暗号化し、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを生成する。メモリカード１２０のコントローラ１４２０は、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａをバスＢＳ４、インタフェース１４２４および端子１４２６を介してインタフェース６０へ出力する（ステップＳ３３４）。

コントローラ４０は、メモリカード１１０からインタフェース６０を介して暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを受理する。そして、コントローラ４０は、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａをインタフェース６０を介してメモリカード１２０へ送信する（ステップＳ３３４）。なお、ステップＳ３３４において、暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａがメモリカード１１０から出力された時点で、メモリカード１１０とメモリカード

１２０との間にライセンスの移動／複製のための通信が確立されたことになる。

図１５を参照して、メモリカード１２０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを受信し、その受信した暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを復号処理部１４１２に与える。復号処理部１４１２は、セッションキー発生部１４１８からのセッションキーＫｓ２ａによって暗号化データ｛Ｋｓ２ｂ／／ＫＰｍｃ４｝Ｋｓ２ａを復号し、セッションキーＫｓ２ｂ、および公開暗号鍵ＫＰｍｃ４を受理する（ステップＳ３３８）。

そうすると、メモリカード１２０のコントローラ１４２０は、メモリ１４１５のログ領域１４１５Ａに含まれる送信ログを初期化し、受理したセッションキーＫｓ２ｂを送信ログに格納する（ステップＳ３４０）。これによって、メモリカード１２０からメモリカード１１０へのライセンスの移動／複製処理を特定するための履歴情報であるセッションキーＫｓ２ｂが送信ログに記録されたことになる。

その後、コントローラ４０は、送信側であるメモリカード１２０のライセンス管理情報から移動／複製の対象となっているライセンスが格納されているエントリ番号を取得し（ステップＳ３４２）、その取得したエントリ番号をインタフェース６０を介してメモリカード１２０へ送信する（ステップＳ３４４）。メモリカード１２０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介してエントリ番号を受信し、その受信したエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂのエントリからライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、再生制御情報ＡＣｐ）と有効フラグとを取得する（ステップＳ３４６）。

コントローラ１４２０は、有効フラグの確認を行なう（ステップＳ３４７）。有効フラグが有効な場合には、次のステップＳ３４８へ進む。有効フラグが無効な場合には、指定されたライセンスが、すでに移動済みであり、ライセンスが使用不能になっていることを示しているためステップＳ３７０へ移行し、移動／複製動作を終了する。ステップＳ３４７において有効フラグが有効な場合、コント

ローラ１４２０は、アクセス制御情報ＡＣｍを確認する（ステップＳ３４８）。つまり、コントローラ１４２０は、取得したアクセス制御情報ＡＣｍに基づいて、最初に、メモリカード１１０へ移動／複製しようとするライセンスが再生回数によって暗号化コンテンツデータの再生ができないライセンスになっていないか否かを確認する。再生回数が残っていない場合（再生回数＝０）、暗号化コンテンツデータをライセンスによって再生することができず、その暗号化コンテンツデータとライセンスとをメモリカード１１０へ移動する意味がないからである。再生することができる場合、移動・複製フラグによって、ライセンスの複製、移動の可否を判断する。

ステップＳ３４８において、暗号化コンテンツデータの再生ができない（再生回数＝０）、または、移動・複製フラグが移動複製禁止（＝０）の場合、アクセス制御情報ＡＣｍによって、複製移動不可と判断し、ステップＳ３７０へ移行し、移動／複製動作は終了する。ステップＳ３４８において、暗号化コンテンツデータの再生ができ（再生回数≠０）、かつ、移動・複製フラグが移動のみ可「＝１」の場合、ライセンスの移動であると判断され、コントローラ１４２０は、メモリ１４１５のライセンス領域１４１５Ｂにおいて指定されたエントリ番号内の有効フラグを無効にし、そのエントリ番号を送信ログに格納する（ステップＳ３５０）。また、暗号化コンテンツデータの再生ができ「再生回数≠０」、かつ、移動・複製フラグが移動複製可「＝３」の場合、ライセンスの複製であると判断され、ステップＳ３５０を行なわずにステップＳ３５２へ移行する。

ステップＳ３４８またはステップＳ３５０の後、メモリカード１２０の暗号処理部１４１７は、復号処理部１４１２によって得られたメモリカード１１０に固有の公開暗号鍵ＫＰｍｃ４によってライセンスを暗号化して暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を生成し（ステップＳ３５２）、暗号処理部１４０６は、暗号処理部１４１７によって暗号化された暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をスイッチ１４４６の接点Ｐｃを介して受取り、復号処理部１４１２によって復号されたセッションキーＫｓ２ｂをスイッチ１４４２の接点Ｐｂを介して受取り、暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ

／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４をセッションキーＫｓ２ｂによって暗号化する。そして、メモリカード１２０のコントローラ１４２０は、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂをバスＢＳ４、インタフェース１４２４、および端子１４２６を介して出力する（ステップＳ３５４）。

このように、ライセンスを移動するときは、ライセンス領域１４１５Ｂの有効フラグを無効にしてから（ステップＳ３５０参照）、ステップＳ３５２の処理を行なうが、ライセンスを複製するときは、複製元と複製先との両方においてライセンスを使用可能にするためにライセンスの有効フラグを無効にするステップＳ３５０を介さずに有効フラグを有効なままステップＳ３５２へ移行するようにしたものである。したがって、ライセンスを移動させたときは、送信側のメモリカード１２０からライセンスを読出すことはできなり、ライセンスを消去した場合と同様な扱いとなる。

図１６を参照して、コントローラ４０は、インタフェース６０を介してメモリカード１２０から暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを受理し、その受理した暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂをメモリカード１１０へ入力する（ステップＳ３５６）。

メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂの入力を受けて、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂを復号処理部１４１２へ与える。そして、復号処理部１４１２は、暗号化データ｛｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４｝Ｋｓ２ｂをバスＢＳ４を介して受取り、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２ｂによって復号し、暗号化データ｛ライセンスＩＤ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４を受理する（ステップＳ３５８）。

その後、コントローラ１４２０の指示によって、暗号化データ｛ライセンスＩ

Ｄ／／コンテンツＩＤ／／Ｋｃ／／ＡＣｍ／／ＡＣｐ｝Ｋｍｃ４は、復号処理部１４０４において、秘密復号鍵Ｋｍｃ４によって復号され、ライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）が受理される（ステップＳ３６０）。

そうすると、コントローラ４０は、受信側であるメモリカード１１０のエントリ管理情報を参照して空きのエントリ番号を取得し、その取得したエントリ番号を移動／複製されたライセンスを格納するためのエントリ番号としてメモリカード１１０に入力する（ステップＳ３６２）。

メモリカード１１０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介してエントリ番号を受取り、その受取ったエントリ番号によって指定されるメモリ１４１５のライセンス領域１４１５Ｂに、ステップＳ３６０において受理したライセンス（ライセンス鍵Ｋｃ、ライセンスＩＤ、コンテンツＩＤ、アクセス制御情報ＡＣｍおよび再生制御情報ＡＣｐ）を格納し、同一エントリの有効フラグを有効にする（ステップＳ３６４）。そして、コントローラ１４２０は、ログ領域１４１５Ａに含まれる受信ログに記録された受信ｓｔａｔｅをＯＦＦにする（ステップＳ３６６）。その後、コントローラ４０は、受信側のメモリカード１１０に対するエントリ管理情報を更新し（ライセンスを記録したエントリを使用中に変更）、受信側のメモリカード１１０に入力する（ステップＳ３６７ａ）。受信側のメモリカード１１０のコントローラ１４２０は、入力されたエントリ管理情報を用いて、メモリ１４１５のデータ領域１４１５Ｃ内のエントリ管理情報を書換える（ステップＳ３６７ｂ）。次に、コントローラ４０は、ライセンスの移動であったかライセンスの複製であったかを判断する（ステップＳ３６８）。複製処理である場合には、ここで、ライセンスの複製の処理を終了する（ステップＳ３７０）。移動処理である場合には、コントローラ４０は、送信側のメモリカード１２０に対するエントリ管理情報を更新し（移動させたライセンスが格納されたエントリを未使用に変更）、送信側のメモリカード１２０に入力する（ステップＳ３６９ａ）。送信側のメモリカード１２０のコントローラ１４２０は、入力されたエントリ管理情報を用いて、メモリ１４１５のデータ領域１４１５Ｃ内のエントリ管理情報を書換える（ステップＳ３６９ｂ）。

そして、ライセンスの移動の処理を終了する（ステップＳ３７０）。

なお、暗号化コンテンツデータのメモリカード１２０からメモリカード１１０への移動／複製は、ライセンスの移動／複製が終了した後、メモリカード１２０のデータ領域１４１５Ｃから暗号化コンテンツデータを読出してメモリカード１１０へ送信することによって行なえば良い。

また、受信側のメモリカード１１０に対しては、移動／複製したライセンスに対するライセンス管理ファイルがすでに記録されている場合には、ライセンス管理ファイルに対してエントリ番号などの書込みを行なうことで対象のライセンス管理ファイルを更新する。また、対象となるライセンス管理ファイルがメモリカード１１０に記録されていない場合には、新たにライセンス管理ファイルを生成し、その生成したライセンス管理ファイルを受信側のメモリカード１１０に記録する。このとき、受信側のメモリカードが図１および図２に示すデータ配信システムにおけるライセンス専用メモリカード５２０であるとすると、ライセンス管理情報はハードディスク５３０に記録される。

このようにして、再生端末１０２に装着されたメモリカード１１０が正規の機器であること、同時に、クラス証明書Ｃｍ３とともに暗号化して送信できた公開暗号鍵ＫＰｍ３が有効であることを確認した上で、正規なメモリカードへの移動要求に対してのみライセンスを移動することができ、不正なメモリカードへの移動を禁止することができる。

また、メモリカードで生成される暗号鍵をやり取りし、お互いが受領した暗号鍵を用いた暗号化を実行して、その暗号化データを相手方に送信することによって、それぞれの暗号化データの送受信においても事実上の相互認証を行なうことができ、ライセンスの移動／複製の動作におけるセキュリティを向上させることができる。

上記においては、メモリカード間における暗号化コンテンツデータのライセンスの移動／複製の動作を説明したが、パーソナルコンピュータ５０のライセンス専用メモリカード５２０からメモリカード１１０へのライセンスの移動／複製も図１４および図１５に示すフローチャートに従って行なうことができる。この移動／複製の動作を用いることによって、配信サーバ１０との通信機能を有さない

再生端末１０２のユーザも、パーソナルコンピュータ５０を介して暗号化コンテンツデータのライセンスをメモリカードに受信することができ、ユーザの利便性は向上する。

また、メモリカード１１０からライセンス専用メモリカード５２０へのライセンスの移動も、図１４～図１６に示すフローチャートに従って行なわれる。つまり、図１において、携帯電話機１００によって配信を受け、メモリカード１１０に格納した暗号化コンテンツデータとライセンスとをパーソナルコンピュータ５０へ退避できることになる。

図１７を参照して、ログ領域１４１５Ａに格納される受信ログと送信ログとについて説明する。ライセンス領域１４１５Ｂには、エントリ番号０～Ｎ－１に対応してライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、再生制御情報ＡＣｐ、および有効フラグが格納されている。有効フラグは、ライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制限情報ＡＣｍ、および再生制御情報ＡＣｐ）の有効性を示すフラグであり、有効フラグが「有効」であるとき、このライセンスを用いて再生を行なったり、このライセンスを他のメモリカード１１０またはライセンス専用メモリカード５２０へ移動／複製できることを意味し、有効フラグが「無効」であるとき、このライセンスを用いて再生できず、かつ、ライセンスを他のメモリカード１１０またはライセンス専用メモリカード５２０へ移動／複製できないことを意味する。すなわち、ライセンスが存在しないことと同等の意味を持つ。移動の対象となったライセンスをメモリカード１２０から取得した後、ライセンス領域１４１５Ｂの有効フラグを無効にしている（図１５のステップＳ３５０）のは、メモリカード１２０からメモリカード１１０へライセンスを移動した後はメモリカード１２０において移動の対象となったライセンスを使用できないようにするためである。

また、ログ領域１４１５Ａには、受信ログ７０および送信ログ８０が記録されている。受信ログ７０は、ライセンスＩＤ７１、セッションキー７２および受信ｓｔａｔｅ７３から成る。また、送信ログ８０は、セッションキー８１およびエントリ番号８２とから成る。受信ログ７０は、メモリカード１１０またはライセ

ンス専用メモリカード５２０が配信サーバ１０、または他のメモリカードやライセンス専用メモリカードからライセンスを受信するときに、その通信履歴を記録しておくものである。送信ログ８０は、ライセンスを他のメモリカードまたはライセンス専用メモリカードへ移動／複製するときに、その通信履歴を記録しておくものである。

なお、ライセンス領域１４１５Ｂおよびログ領域１４１５Ａは、ＴＲＭ領域に設けられていることが好ましい。また、ログ領域１４１５Ａ、ライセンス領域１４１５Ｂおよびデータ領域１４１５Ｃは、メモリ１４１５として１つの領域に含まれている必要はなく、それぞれ、独立した構成であってもよい。さらに、ログ領域１４１５Ａに記録された受信ログ７０および送信ログ８０は、外部から書換えができないように構成されていなければならない。

メモリカード１１０またはライセンス専用メモリカード５２０が配信サーバ１０からライセンスを受信するとき、ライセンスＩＤ、および自己のセッションキー発生部１４１８で生成したセッションキーを受信ログ７０に記録し（図９のステップＳ１３０、およびステップＳ１３６参照）、受信ログ７０に記録された受信ｓｔａｔｅ７３をＯＮにしている（図９のステップＳ１３６参照）。また、メモリカード１１０またはライセンス専用メモリカード５２０が他のメモリカードまたはライセンス専用メモリカードからライセンスを受信するときも、同様に、ライセンスＩＤ、および自己のセッションキー発生部１４１８で生成したセッションキーを受信ログ７０に記録し（図１４のステップＳ３２６、およびステップＳ３３２参照）、受信ｓｔａｔｅをＯＮにしている（図１４のステップＳ３３２参照）。

一方、図１３におけるメモリカード１２０からメモリカード１１０へのライセンスの移動において、受信側のメモリカード１１０から送信されたセッションキーおよび移動／複製の対象となったライセンスのエントリ番号を送信ログ８０に記録する（図１５のステップＳ３４０およびステップＳ３５０参照）。メモリカード１２０からメモリカード１１０への移動／複製処理においては、受信ログ７０のセッションキー７２と送信ログ８０のセッションキー８１とには同じセッションキーＫｓ２ｂが記録される（図１４のステップＳ３３２および図１５のステ

ップＳ３４０参照）。したがって、メモリカード１２０からメモリカード１１０へのライセンスの移動／複製の途中において通信が切断されたとき、メモリカード１２０の送信ログ８０に記録されたセッションキー８１が、メモリカード１１０の受信ログ７０に記録されたセッションキー７２に一致することを確認すれば、メモリカード１２０からメモリカード１１０へのライセンスの移動／複製処理を特定することができる。

また、メモリカード１１０へのライセンスの配信においては、メモリカード１１０が、メモリカード１１０において生成したセッションキーＫｓ２を配信サーバ１０へ送信すると、受信ｓｔａｔｅ７３がＯＮされ（図９のステップＳ１３８）、配信サーバ１０から受信したライセンスをメモリ１４１５のライセンス領域１４１５Ｂに格納した後に受信ｓｔａｔｅ７３がＯＦＦされる（図１０のステップＳ１６２）。したがって、ステップ１３８からステップＳ１６２までの間、受信ｓｔａｔｅ７３は、ＯＮされたままであるので、何らかの原因によって通信が切断されたとき、メモリカード１１０の受信ログ７０から受信ｓｔａｔｅ７３を読出し、受信ｓｔａｔｅ７３がＯＮかＯＦＦかを調べれば、どの状態で通信が切断されたのかが解かる。つまり、読出した受信ｓｔａｔｅ７３がＯＮであればライセンスがメモリカード１１０のライセンス領域１４１５Ｂに格納されていないときに通信が切断されたことになり、受信ｓｔａｔｅ７３がＯＦＦであれば、ライセンスがメモリカード１１０のライセンス領域１４１５Ｂに格納された後に通信が切断されたことになる。

また、メモリカード１２０からメモリカード１１０へのライセンスの移動／複製処理においても図１４のステップＳ３３２から図１６のステップＳ３６４までの間、受信ｓｔａｔｅ７３がＯＮされたままであるので、この場合にもライセンスの配信の場合と同じことが言える。

［復元］

図１４～図１６に示すフローチャートに従ってライセンスをメモリカード１２０からメモリカード１１０へ移動する途中で通信が切断されたときに、メモリカード１２０において移動の対象となったライセンスを復元する動作を図１８および図１９を参照して説明する。すなわち、図１５のステップＳ３４８において

「移動」と判断された後、ステップＳ３５０から図１６のステップＳ３６４の間に通信が中断する等の理由によって移動処理が中断した場合、ライセンスが送信側のメモリカード１２０および受信側のメモリカード１１０のいずれにも存在しな状態になり、ライセンスの消失が存在する。この場合に、送信側のメモリカード１２０において移動の対象となったライセンスを復元することにしたものである。この場合も図１３に示す系を想定する。

図１８を参照して、携帯電話機１００の操作パネル１１０８から復元リクエストが入力されると（ステップＳ４００）、コントローラ４０は、認証データの送信要求をインタフェース６０を介してメモリカード１１０へ送信する（ステップＳ４０２）。そして、メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４およびバスＢＳ４を介して認証データの送信要求を受信する（ステップＳ４０４）。

コントローラ１４２０は、認証データの送信要求を受信すると、認証データ保持部１４００から認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４を介して読出し、その読出した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４、インタフェース１４２４および端子１４２６を介してコントローラ４０へ出力する（ステップＳ４０６）。そして、コントローラ４０は、インタフェース６０を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受取り、インタフェース６０を介してメモリカード１２０へ認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを送信する（ステップＳ４０８）。

そうすると、メモリカード１２０のコントローラ１４２０は、端子１４２６およびインタフェース１４２４を介して認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａを受信し、その受信した認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａをバスＢＳ４を介して復号処理部１４０８へ与える。そして、復号処理部１４０８は、ＫＰａ保持部１４１４からの公開認証鍵ＫＰａによって認証データ｛ＫＰｍ３／／Ｃｍ３｝ＫＰａの復号処理を実行する（ステップＳ４１０）。コントローラ１４２０は、復号処理部５２０８における復号処理結果から、処理が正常に行なわれたか否か、すなわち、メモリカード１１０が正規のメモリカードであって、メモリカード１１０から正規の機関でその正当性を証明するための暗号を施した認証デー

タを受信したか否かを判断する認証処理を行なう（ステップＳ４１２）。正当な認証データであると判断された場合、コントローラ１４２０は、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を承認し、受理する。そして、次の処理（ステップＳ４１４）へ移行する。正当な認証データでない場合には、非承認とし、クラス公開暗号鍵ＫＰｍ３およびクラス証明書Ｃｍ３を受理しないで処理を終了する（ステップＳ４６２）。

認証の結果、正当な認証データを持つメモリカードを備えるメモリカードからの認証データであることが確認されると、メモリカード１２０において、コントローラ１４２０は、セッションキー発生部１４１８を制御し、セッションキー発生部１４１８は、移動のためのセッションキーＫｓ２ｃを生成する（ステップＳ４１４）。セッションキーＫｓ２ｃは、復号処理部１４０８によって得られたメモリカード１１０に対応するクラス公開暗号鍵ＫＰｍ３によって、暗号処理部１４１０によって暗号化される。そして、コントローラ１４２０は、バスＢＳ４を介して暗号化データ｛Ｋｓ２ｃ｝Ｋｍ３を取得し、バスＢＳ４、インタフェース１４２４および端子１４２６を介して暗号化データ｛Ｋｓ２ｃ｝Ｋｍ３を出力する（ステップＳ４１６）。

コントローラ４０は、インタフェース６０を介して暗号化データ｛Ｋｓ２ｃ｝Ｋｍ３を送信側から受理し（ステップＳ４１８）、その受理した暗号化データ｛Ｋｓ２ｃ｝Ｋｍ３をインタフェース６０を介してメモリカード１１０へ入力する（ステップＳ４２０）。この入力によってメモリカード１１０に対して受信ログの出力を命令することになる。

メモリカード１１０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛Ｋｓ２ｃ｝Ｋｍ３を受理し、暗号化データ｛Ｋｓ２ｃ｝Ｋｍ３を復号処理部１４２２へ与える。復号処理部１４２２は、Ｋｍ保持部１４２１からの秘密復号鍵Ｋｍ３によって暗号化データ｛Ｋｓ２ｃ｝Ｋｍ３を復号してセッションキーＫｓ２ｃを受理する（ステップＳ４２２）。コントローラ１４２０は、メモリ１４１５のログ領域１４１５Ａの受信ログ７０からセッションキーＫｓ２ｂを取得し、その取得したセッションキーＫｓ２ｂをスイッチ１４４６の接点Ｐｆを介して暗号処理部１４０６に与え

る。暗号処理部１４０６は、復号処理部１４２２によって復号されたセッションキーＫｓ２ｃをスイッチ１４４２の接点Ｐａを介して受取り、セッションキーＫｓ２ｂをセッションキーＫｓ２ｃによって暗号化して暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ｃを生成する（ステップＳ４２４）。そして、コントローラ１４２０は、受信ログ７０からライセンスＩＤ、および受信ｓｔａｔｅを取得し、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅを生成し、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅのハッシュ値ｈａｓｈを求める（ステップＳ４２６）。つまり、コントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅに対する署名を行なう。

その後、コントローラ１４２０は、ハッシュ値ｈａｓｈをスイッチ１４４６の接点Ｐｆを介して暗号処理部１４０６に与え、暗号処理部１４０６は、ハッシュ値ｈａｓｈをセッションキーＫｓ２ｃによって暗号化を行ない、暗号化データ｛ｈａｓｈ｝Ｋｓ２ｃを生成する（ステップＳ４２８）。そして、コントローラ１４２０は、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ｃを生成して出力する（ステップＳ４３０）。つまり、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅに対する署名をさらにセッションキーＫｓ２ｃによって暗号化することによってライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅに対する署名が改竄されるのを防止している。

コントローラ４０は、インタフェース６０を介してライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ｃを受信し、受信ｓｔａｔｅの確認を行なう（ステップＳ４３２）。受信ｓｔａｔｅがＯＦＦであれば、メモリカード１２０からメモリカード１１０へライセンスが移動／複製された後に通信が切断されたことを意味するので、ライセンスの復元動作は終了する（ステップＳ４６２）。ステップＳ４３２において、受信ｓｔａｔｅがＯＮであること、つまり、メモリカード１２０からメモリカード１１０へのライセンスの移動／複製の途中で通信が切断されたことが確認されると、コントローラ４０は、ライセンスＩＤの確認を行なう。すなわち、メモリカード１１０から読出したライセンスＩＤ（ステップＳ４２６）が、メモリカード１２０が保持するライ

センスＩＤに一致するか否かを確認する。そして、２つのライセンスＩＤが不一致であるとき、移動／複製の対象となったライセンスを特定できないので、ライセンスの復元動作は終了する（ステップＳ４６２）。ステップＳ４３４において、２つのライセンスＩＤが一致すると、コントローラ４０は、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ｃをメモリカード１２０へ入力する（ステップＳ４３６）。

図１９を参照して、メモリカード１２０のコントローラ１４２０は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介してライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅ／／｛ｈａｓｈ｝Ｋｓ２ｃを受理し（ステップＳ４３８）、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅのハッシュ値ｈａｓｈを求める（ステップＳ４４０）。そして、コントローラ１４２０は、受理した暗号化データ｛ｈａｓｈ｝Ｋｓ２ｃを復号処理部１４１２へ与え、復号処理部１４１２は、暗号化データ｛ｈａｓｈ｝Ｋｓ２ｃをセッションキー発生部１４１８からのセッションキーＫｓ２ｃによって復号し、メモリカード１１０において生成されたハッシュ値ｈａｓｈを受理する（ステップＳ４４２）。

その後、メモリカード１２０のコントローラ１４２０は、自ら求めたハッシュ値ｈａｓｈ（ステップＳ４４０）が、メモリカード１１０において生成されたハッシュ値ｈａｓｈに一致するか否かの確認を行なう（ステップＳ４４４）。そして、２つのハッシュ値ｈａｓｈが不一致であるとき、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅに対する署名が改竄されていることになるので、ライセンスの復元処理は終了する（ステップＳ４６２）。ステップＳ４４４において、２つのハッシュ値ｈａｓｈが一致しているとき、コントローラ１４２０は、受信ｓｔａｔｅの確認を行なう（ステップＳ４４６）。受信ｓｔａｔｅがＯＦＦであれば、メモリカード１２０からメモリカード１１０へライセンスが移動／複製された後に通信が切断されたことを意味するので、ライセンスの復元動作は終了する（ステップＳ４６２）。ステップＳ４４６において、受信ｓｔａｔｅがＯＮであること、つまり、メモリカード１２０からメモリカード１１０へのライセンスの移動／複製の途中で通信が切断されたことが確認されると、コント

ローラ１４２０は、受理した暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ｃを復号処理部１４１２へ与える。そして、復号処理部１４１２は、暗号化データ｛Ｋｓ２ｂ｝Ｋｓ２ｃを、セッションキー発生部１４１８からのセッションキーＫｓ２ｃによって復号し、セッションキーＫｓ２ｂを受理する（ステップＳ４４８）。

その後、コントローラ１４２０は、メモリ１４１５のログ領域１４１５Ａの送信ログ８０に記録されたセッションキーＫｓ２ｂを読出し、その読出したセッションキーＫｓ２ｂがメモリカード１１０から受信したセッションキーＫｓ２ｂに一致するか否かを比較する（ステップＳ４５０）。２つのセッションキーが不一致であるときは、メモリカード１１０から受信したセッションキーＫｓ２ｂは、異なる移動／複製処理を特定するセッションキーであるので、ライセンスの復元処理は終了する（ステップＳ４６２）。ステップＳ４５０において、２つのセッションキーが一致したとき、コントローラ１４２０は、メモリ１４１５のログ領域１４１５Ａの送信ログにエントリ番号が記録されているか否かを確認し（ステップＳ４５２）、エントリ番号が記録されていなければライセンスの移動／複製を行なっていなかったことになるので、ライセンスの復元処理は終了する（ステップＳ４６２）。ステップＳ４５２において、送信ログにエントリ番号が記録されている場合、コントローラ１４２０は、送信ログ内のエントリ番号を読出し、その読出したエントリ番号によって指定された領域に格納されているライセンスＩＤをライセンス領域１４１５Ｂから取得する（ステップＳ４５４）。

そして、コントローラ１４２０は、メモリカード１１０から受信したライセンスＩＤとメモリカード１２０のライセンス領域１４１５Ｂから取得したライセンスＩＤとを比較し（ステップＳ４５６）、２つのライセンスＩＤが不一致であるとき、ライセンスの復元処理は終了する（ステップＳ４６２）。ステップＳ４５６において、２つのライセンスＩＤが一致したとき、コントローラ１４２０は、ログ領域１４１５Ａの送信ログに記録されたエントリ番号によって指定されたライセンスの有効フラグを無効から有効にする（ステップＳ４５８）。これによって、ライセンスの送信側においてライセンスが復元される。その後、メモリカード１２０のコントローラ１４２０は、ログ領域１４１５Ａの送信ログを初期化し（ステップＳ４６０）、ライセンスの復元処理が終了する（ステップＳ４６

２）。

このように、ライセンスの移動／複製を行なっていた相手であること、その行なっていた移動／複製処理が特定されること等を条件としてライセンスの復元を送信側において行なうことができる。また、ライセンスＩＤ／／｛Ｋｓ２ｂ｝Ｋｓ２ｃ／／受信ｓｔａｔｅに対する署名をメモリカード１１０（受信先）とメモリカード１２０（送信元）とで行ない、両者の署名が一致することを確認してライセンスの復元処理を続行することによって安全なライセンスの復元を提供することができる。

なお、上記においては、メモリカード１２０からメモリカード１１０へのライセンスの移動およびメモリカード１２０からメモリカード１１０へのライセンスの移動動作におけるライセンスの復元について説明したが、メモリカード１１０からメモリカード１２０へのライセンスの移動および復元についても、図１４～図１６、図１８および図１９に示すフローチャートに従って行なわれる。また、メモリカード１１０，１２０以外の複数のメモリカードのいずれかからのライセンスの移動および復元についても、図１４～図１６、図１８、および図１９に示すフローチャートに従って行なわれる。

［再生］

上述したように、携帯電話機１００または再生端末１０２に装着されたメモリカード１１０は、配信サーバ１０から、直接、暗号化コンテンツデータおよびライセンスを受信できる。また、メモリカード１１０は、パーソナルコンピュータ５０が配信サーバ１０からハード的に取得した暗号化コンテンツデータおよびライセンスを、「移動」という概念によってパーソナルコンピュータ５０から受信できる。

このように、メモリカード１１０は、各種の方法によって暗号化コンテンツデータおよびライセンスを受信する。そこで、次に、これらの各種の方法によってメモリカードが受信した暗号化コンテンツデータの再生について説明する。

図２０は、メモリカード１１０が受信したコンテンツデータの再生端末１０２における再生動作を説明するためのフローチャートである。なお、図２０における処理以前に、再生端末１０２のユーザは、メモリカード１１０のデータ領域１

４１５Ｃに記録されている再生リストに従って、再生するコンテンツ（楽曲）を決定し、コンテンツファイルを特定し、ライセンス管理ファイルを取得していることを前提として説明する。

図２０を参照して、再生動作の開始とともに、再生端末１００のユーザから操作パネル１１０８を介して再生リクエストが再生端末１００にインプットされる（ステップＳ７００）。そうすると、コントローラ１１０６は、バスＢＳ３を介して認証データの出力要求をコンテンツ再生回路１５５０に行ない（ステップＳ７０２）、コンテンツ再生回路１５５０は認証データの出力要求を受信する（ステップＳ７０４）。そして、認証データ保持部１５００は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを出力し（ステップＳ７０６）、コントローラ１１０６は、メモリカードインタフェース１２００を介してメモリカード１１０へ認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを入力する（ステップＳ７０８）。

そうすると、メモリカード１１０は、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを受理し、復号処理部１４０８は、受理した認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａを、ＫＰａ保持部１４１４に保持された公開認証鍵ＫＰａによって復号し（ステップＳ７１０）、コントローラ１４２０は復号処理部１４０８における復号処理結果から、認証処理を行なう。すなわち、認証データ｛ＫＰｐ１／／Ｃｐ１｝ＫＰａが正規の認証データであるか否かを判断する認証処理を行なう（ステップＳ７１２）。復号できなかった場合、ステップＳ７４６へ移行し、再生動作は終了する。認証データを復号できた場合、コントローラ１４２０は、セッションキー発生部１４１８を制御し、セッションキー発生部１４１８は、再生セッション用のセッションキーＫｓ２を発生させる（ステップＳ７１２）。そして、暗号処理部１４１０は、セッションキー発生部１４１８からのセッションキーＫｓ２を、復号処理部１４０８で復号された公開暗号鍵ＫＰｐ１によって暗号化した暗号化データ｛Ｋｓ２｝Ｋｐ１をバスＢＳ３へ出力する。そうすると、コントローラ１４２０は、インタフェース１４２４および端子１４２６を介してメモリカードインタフェース１２００へ暗号化データ｛Ｋｓ２｝Ｋｐ１を出力する（ステップＳ７１４）。再生端末１０２のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ２｝Ｋｐ１を取得する。

そして、コントローラ１１０６は、暗号化データ｛Ｋｓ２｝Ｋｐ１をバスＢＳ３を介してコンテンツ再生回路１５５０の復号処理部１５０４へ与え（ステップＳ７１６）、復号処理部１５０４は、Ｋｐ保持部１５０２から出力された、公開暗号鍵ＫＰｐ１と対になっている秘密復号鍵Ｋｐ１によって暗号化データ｛Ｋｓ２｝Ｋｐ１を復号し、セッションキーＫｓ２を暗号処理部１５０６へ出力する（ステップＳ７１８）。そうすると、セッションキー発生部１５０８は、再生セッション用のセッションキーＫｓ３を発生させ、セッションキーＫｓ３を暗号処理部１５０６へ出力する（ステップＳ７２０）。暗号処理部１５０６は、セッションキー発生部１５０８からのセッションキーＫｓ３を復号処理部１５０４からのセッションキーＫｓ２によって暗号化して暗号化データ｛Ｋｓ３｝Ｋｓ２を出力し（ステップＳ７２２）、コントローラ１１０６は、バスＢＳ３およびメモリカードインタフェース１２００を介して暗号化データ｛Ｋｓ３｝Ｋｓ２をメモリカード１１０へ出力する（ステップＳ７２４）。

そうすると、メモリカード１１０の復号処理部１４１２は、端子１４２６、インタフェース１４２４、およびバスＢＳ４を介して暗号化データ｛Ｋｓ３｝Ｋｓ２を入力する。復号処理部１４１２は、セッションキー発生部１４１８によって発生されたセッションキーＫｓ２によって暗号化データ｛Ｋｓ３｝Ｋｓ２を復号して、再生端末１０２で発生されたセッションキーＫｓ３を受理する（ステップＳ７２６）。

再生端末１０２のコントローラ１１０６は、メモリカード１１０から事前に取得した再生リクエスト曲のライセンス管理ファイルからライセンスの格納されているエントリ番号を取得し（ステップＳ７２８）、メモリカードインタフェース１２００を介してメモリカード１１０へ取得したエントリ番号と再生許諾要求を出力する（ステップＳ７３０）。

メモリカード１１０のコントローラ１４２０は、エントリ番号と再生許諾要求とを受理し、エントリ番号によって指定された領域に格納されたライセンスおよび有効フラグを取得する（ステップＳ７３２）。そして、コントローラ１４２０は、有効フラグを確認する（ステップＳ７３３）。ステップＳ７３３において、有効フラグが「無」の場合、指定されたエントリにライセンスが存在しないの

で、再生動作が終了する（ステップＳ７４６）。ステップＳ７３３において、有効フラグが「有効」の場合、指定されたエントリにライセンスが存在するので次のステップＳ７３４へ進む。

そして、コントローラ１４２０は、アクセス制限情報ＡＣｍを確認する（ステップＳ７３４）。

ステップＳ７３４においては、メモリのアクセスに対する制限に関する情報であるアクセス制限情報ＡＣｍを確認することにより、具体的には、再生回数を確認することにより、既に再生不可の状態である場合には再生動作を終了し、アクセス制限情報の再生回数に制限がある場合にはアクセス制限情報ＡＣｍの再生回数を変更した（ステップＳ７３６）後に次のステップに進む（ステップＳ７３８）。一方、アクセス制限情報ＡＣｍの再生回数によって再生が制限されていない場合においては、ステップＳ７３６はスキップされ、アクセス制限情報ＡＣｍの再生回数は変更されることなく処理が次のステップ（ステップＳ７３８）に進行される。

ステップＳ７３４において、当該再生動作において再生が可能であると判断された場合には、メモリ１４１５のライセンス領域１４１５Ｂに記録された再生リクエスト曲のライセンス鍵Ｋｃおよび再生制御情報ＡＣｐがバスＢＳ４上に出力される（ステップＳ７３８）。

得られたライセンス鍵Ｋｃと再生制御情報ＡＣｐは、切換スイッチ１４４６の接点Ｐｆを介して暗号処理部１４０６に送られる。暗号処理部１４０６は、切換スイッチ１４４２の接点Ｐｂを介して復号処理部１４１２より受けたセッションキーＫｓ３によって切換スイッチ１４４６を介して受けたライセンス鍵Ｋｃと再生制御情報ＡＣｐとを暗号化し、暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３をバスＢＳ４に出力する（ステップＳ７３８）。

バスＢＳ４に出力された暗号化データは、インタフェース１４２４、端子１４２６、およびメモリカードインタフェース１２００を介して再生端末１０２に送出される。

再生端末１０２においては、メモリカードインタフェース１２００を介してバスＢＳ３に伝達される暗号化データ｛Ｋｃ／／ＡＣｐ｝Ｋｓ３を復号処理部１５

１０によって復号処理を行ない、ライセンス鍵Ｋｃおよび再生制御情報ＡＣｐを受理する（ステップＳ７４０，Ｓ７４２）。復号処理部１５１０は、ライセンス鍵Ｋｃを復号処理部１５１６に伝達し、再生制御情報ＡＣｐをバスＢＳ３に出力する。

コントローラ１１０６は、バスＢＳ３を介して、再生制御情報ＡＣｐを受理して再生の可否の確認を行なう（ステップＳ７４４）。

ステップＳ７４４においては、再生制御情報ＡＣｐによって再生不可と判断される場合には、再生動作は終了される。

ステップＳ７４４において再生可能と判断された場合、コントローラ１１０６は、メモリカードインタフェース１２００を介してメモリカード１１０に暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを要求する。そうすると、メモリカード１１０のコントローラ１４２０は、メモリ１４１５から暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ４、インタフェース１４２４、および端子１４２６を介してメモリカードインタフェース１２００へ出力する。

再生端末１０２のコントローラ１１０６は、メモリカードインタフェース１２００を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを取得し、バスＢＳ３を介して暗号化コンテンツデータ｛Ｄｃ｝Ｋｃをコンテンツ再生回路１５５０へ与える。

そして、コンテンツ再生回路１５５０の復号処理部１５１６は、暗号化コンテンツデータ｛Ｄｃ｝Ｋｃを復号処理部１５１０から出力されたライセンス鍵Ｋｃによって復号してコンテンツデータＤｃを取得する。

そして、復号されたコンテンツデータＤｃは音楽再生部１５１８へ出力され、音楽再生部１５１８は、コンテンツデータを再生し、ＤＡ変換器１５１９はディジタル信号をアナログ信号に変換して端子１５３０へ出力する。そして、音楽データは端子１５３０から外部出力装置を介してヘッドホーン１３０へ出力されて再生される。これによって再生動作が終了する（ステップＳ７４６）。

パーソナルコンピュータ５０のライセンス専用メモリカード５２０における暗号化コンテンツデータの再生動作も図２０に示すフローチャートに従って行なわれる。

また、パーソナルコンピュータ５０は、ライセンス専用メモリカード５２０を装着し、その装着したライセンス専用メモリカード５２０にライセンスを記録するものとして説明したが、ライセンス専用メモリカード５２０に代えて、メモリカード１１０を装着し、その装着したメモリカードにライセンスのみを管理させることも可能である。

さらに、メモリカード１１０を携帯電話機１００またはデータ再生端末１０２に装着した場合と同様に、暗号化コンテンツデータおよびライセンス管理情報をライセンス専用メモリカード５２０のデータ領域１４１５Ｃに記録して用いることも可能である。

また、さらに、ライセンス専用メモリカード５２０に代えて、データ領域１４１５Ｃを備えないライセンス専用メモリカードやライセンス専用の記録デバイス（半導体チップ）などを用いることも可能である。この場合、エントリ管理情報はハードディスク５３０に記録される。

また、さらに、パーソナルコンピュータ５０においては、暗号アルゴリズムを備え、ソフトウェアによって耐タンパモジュールを実現したライセンス管理プログラムによってライセンス専用メモリカード５２０の機能を実現するこも可能である。この場合、ログ領域１４１５Ａおよびライセンス領域１４１５Ｂは、ハードディスク５３０に設けられ、ライセンス管理プログラムによって独自に暗号化され、ライセンス管理プログラム以外からアクセスしても、内容が確認および書換えができないように構成される。また、パーソナルコンピュータ５０のハードディスク５３０またはコントローラ５１０に関連付けて記録され、パーソナルコンピュータ５０においてのみアクセス可能となるように構成される。さらに、図１４～図１６に示すフローチャートによらない移動／複製されたライセンスは、無効となるように構成される。

本発明の実施の形態によれば、送信元のメモリカードは、ライセンスの移動を有効フラグによって管理し、ライセンスの移動の途中で通信が切断されたとき、ライセンスの移動を行なっていた相手であること等を確認して有効フラグを有効にするので、送信元におけるライセンスの復元を容易に行なうことができる。

上記の説明において、ライセンスを移動させるとき有効フラグを用いることに

より送信側のメモリカードにおいて移動対象となるライセンスを復元でき、かつ、使用不能となる状態を実現した。この他に、たとえば、移動の対象となるライセンスをメモリカードのメモリ１４１５のログ領域１４１５Ａの送信ログに１ライセンス分の待避ライセンスを格納できるようにログ領域１４１５Ａを拡張し、移動の対象となるライセンスを送信ログに待避して、移動するライセンスが記録されているエントリ内を消去することで実現可能である。この場合、エントリごとに設けられる有効フラグは必要ない。

この構成の場合、移動処理においては、送信側のメモリカード１１０では図１５のステップＳ３５０において、指定されたエントリ番号および指定されたエントリ番号内のライセンスをログ領域１４１５Ａの送信ログに格納し、指定されたエントリ番号内のライセンスを消去する。受信側のメモリカード１２０では、ステップＳ３６４を、「ライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐ）をエントリ番号で指定されたエントリに格納する」ように変更すればよい。さらに、復元処理において、図１９のステップＳ４５８を、「待避ライセンスを送信ログ内のエントリ番号で示されるエントリに複製する」ように変更すればよい。

同様に、配信処理の各処理において、有効フラグの設定および確認を行なう必要がなくなる。この場合、図１０のステップＳ１６０を、「ライセンス（ライセンスＩＤ、コンテンツＩＤ、ライセンス鍵Ｋｃ、アクセス制御情報ＡＣｍ、および再生制御情報ＡＣｐ）をエントリ番号で指定されたエントリに格納する」ように変更する。再生処理では、有効フラグが運用されていないので、図２０のステップＳ７３３の処理は必要なくなる。

上記においては、暗号化コンテンツデータを復号するためのライセンスを例にして、ライセンスの復元処理について説明したが、本発明においては、復元の対象となるものは暗号化コンテンツデータを復号するためのライセンスに限らず、個人情報、およびクレジットカードの情報等の同時に２個以上存在してはいけないデータが復元の対象となる。このようなデータについても、上述した各処理を行なうことができる。

今回開示された実施の形態はすべての点で例示であって制限的なものではない

と考えられるべきである。本発明の範囲は、上記した実施の形態の説明ではなくて特許請求の範囲によって示され、特許請求の範囲と均等の意味および範囲内でのすべての変更が含まれることが意図される。

産業上の利用可能性

本発明によれば、送信元のメモリカードは、ライセンスの移動を有効フラグによって管理し、ライセンスの移動の途中で通信が切断されたとき、ライセンスの移動を行なっていた相手であること等を確認して有効フラグを有効にするので、送信元におけるライセンスの復元を容易に行なうことができる。したがって、本発明は、ライセンスの移動中に通信が切断されても、その移動と対象となったライセンスを復元可能なデータ記録装置に適用される。

請求の範囲

１．一義的にのみ存在することが許容される独自データを他のデータ記録装置（１１０，５２０）へ移動するデータ記録装置（１２０）であって、

前記他のデータ記録装置（１１０，５２０）への前記独自データの移動処理を特定するための第１の履歴情報（８１）を保持する履歴情報保持部（１４１５Ａ，８０）と、

前記独自データを保持する独自データ保持部（１４１５Ｂ）と、

制御部（１４２０）とを備え、

前記制御部（１４２０）は、

前記独自データの前記他のデータ記録装置（１１０，５２０）への移動に対して前記独自データの外部への出力が不可能な状態に変更し、

前記独自データの復元要求に応じて、前記他のデータ記録装置（１１０，５２０）との通信状態を示す前記他のデータ記録装置（１１０，５２０）に保持された通信情報（７３）と前記他のデータ記録装置（１１０，５２０）に保持された前記移動処理を特定するための第２の履歴情報（７２）とを前記他のデータ記録装置（１１０，５２０）から受信し、前記通信情報（７３）に基づいて前記他のデータ記録装置（１１０，５２０）との通信状態を確認し、前記通信情報（７３）が前記移動の途中を示すとき前記第２の履歴情報（７２）が前記第１の履歴情報（８１）に一致するか否かを判定し、前記第２の履歴情報（７２）が前記第１の履歴情報（８１）に一致するとき前記独自データの外部への出力が可能な状態に復元する、データ記録装置。

２．前記独自データ保持部（１４１５Ｂ）は、前記独自データの一部または全てを外部へ出力可能か出力不可かを示す出力可否フラグをさらに保持し、

前記制御部（１４２０）は、

前記独自データの前記他のデータ記録装置（１１０，５２０）への移動に対して前記出力可否フラグを出力不可に設定し、

前記独自データの復元時、前記出力可否フラグを出力可能に設定する、請求項１に記載のデータ記録装置。

３．前記履歴情報保持部（１４１５Ａ，８０）は、前記移動の対象となった独自データを外部へ出力不可能な状態でさらに保持し、

前記制御部（１４２０）は、

前記独自データの前記他のデータ記録装置（１１０，５２０）への移動に対して前記移動の対象となった独自データを前記履歴情報保持部（１４１５Ａ，８０）に与え、前記独自データ保持部から前記移動の対象となった独自データを消去し、

前記独自データの復元時、前記履歴情報保持部（１４１５Ａ，８０）に保持された独自データを前記独自データ保持部に書込む、請求項１に記載のデータ記録装置。

４．前記第１の履歴情報（８１）は、前記移動のための通信確立時に前記他のデータ記録装置（１１０，５２０）で生成され、かつ、前記他のデータ記録装置（１１０，５２０）から受信された第１のセッション鍵であり、

前記第２の履歴情報（７２）は、前記移動のための通信確立時に前記他のデータ記録装置（１１０，５２０）で生成され、かつ、前記他のデータ記録装置（１１０，５２０）に保持された前記第１のセッション鍵と同じ第２のセッション鍵である、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

５．電子署名により前記通信情報（７３）と前記第２の履歴情報（７２）との正当性を確認する署名確認手段（１４２０）をさらに備え、

前記制御部（１４２０）は、さらに、前記通信情報（７３）と前記第２の履歴情報（７２）とに対する電子署名を前記通信情報（７３）および前記第２の履歴情報（７２）とともに前記他のデータ記録装置（１１０，５２０）から受信し、前記署名確認手段（１４２０）によって前記通信情報（７３）と前記第２の履歴情報（７２）の正当性が確認されたとき、前記通信状態を確認し、かつ、前記第１の履歴情報（８１）と前記第２の履歴情報（７２）との一致を確認する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

６．前記他のデータ記録装置（１１０，５２０）との通信を特定するためのセッション鍵を生成するセッション鍵生成部（１４１８）と、

前記セッション鍵生成部（１４１８）が生成したセッション鍵によって暗号化

されたデータを復号する復号部（１４１２）とをさらに備え、

前記独自データの復元時、

前記セッション鍵生成部（１４１８）は、前記独自データの復元のための通信を特定する第３のセッション鍵を生成し、

前記制御部（１４２０）は、前記第３のセッション鍵を前記他のデータ記録装置（１１０，５２０）へ送信し、前記第３のセッション鍵によって暗号化された第２の履歴情報（７２）を前記他のデータ記録装置（１１０，５２０）から受信する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

７．前記他のデータ記録装置（１１０，５２０）との通信を特定するためのセッション鍵を生成するセッション鍵生成部（１４１８）と、

前記セッション鍵生成部（１４１８）が生成したセッション鍵によって暗号化されたデータを復号する復号部（１４１２）とをさらに備え、

前記独自データの復元時、

前記セッション鍵生成部（１４１８）は、前記独自データの復元のための通信を特定する第３のセッション鍵を生成し、

前記制御部（１４２０）は、前記第３のセッション鍵を前記他のデータ記録装置（１１０，５２０）へ送信し、前記第３のセッション鍵によって暗号化された第２の履歴情報（７２）と、前記第３のセッション鍵によって暗号化された前記電子署名のデータとを前記他のデータ記録装置（１１０，５２０）から受信する、請求項５に記載のデータ記録装置。

８．前記履歴情報保持部（１４１５Ａ，８０）は、前記移動の対象となった独自データに含まれる第１のデータ特定情報を前記第１の履歴情報（８１）とともに保持し、

前記制御部（１４２０）は、さらに、前記他のデータ記録装置（１１０，５２０）から受信する前記移動の対象となった前記第２のデータ特定情報が前記第１のデータ特定情報に一致するか否かを判定し、前記第２のデータ特定情報が前記第１のデータ特定情報に一致するとき、前記通信情報（７３）を確認し、かつ、前記第１の履歴情報（８１）と前記第２の履歴情報（７２）との一致を確認する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

９．電子署名により前記通信情報（７３）と前記第２の履歴情報（７２）と前記第２のデータ特定情報との正当性を確認する署名確認手段（１４２０）をさらに備え、

前記制御部（１４２０）は、さらに、前記通信情報（７３）と前記第２の履歴情報（７２）と前記第２のデータ特定情報とに対する電子署名を、前記通信情報（７３）と前記第２の履歴情報（７２）と前記第２のデータ特定情報とともに受信し、前記署名確認手段（１４２０）によって前記通信情報（７３）と前記第２の履歴情報（７２）と前記第２のデータ特定情報の正当性が確認されたとき、前記第２のデータ特定情報と前記第１のデータ特定情報との一致を確認し、かつ、前記通信情報（７３）を確認し、前記第１の履歴情報（８１）と前記第２の履歴情報（７２）との一致を確認する、請求項８に記載のデータ記録装置。

１０．前記他のデータ記録装置（１１０，５２０）または前記他のデータ記録装置（１１０，５２０）と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報を保持する通信情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴情報保持部（１４１５Ａ，７０）とをさらに備え、

前記制御部（１４２０）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するとき、前記第３の履歴情報を前記もう１つの履歴情報保持部（１４１５Ａ，７０）に記録し、外部からの履歴情報の出力要求に応じて前記通信情報（７３）と前記第３の履歴情報とを出力する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

１１．前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成部（１４１８）をさらに備え、

前記セッション鍵生成部（１４１８）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するための通信を特定する第４のセ

ッション鍵を生成し、

前記制御部（１４２０）は、前記移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つのデータ記録装置から受信する通信の確立時、前記第４のセッション鍵を前記他のデータ記録装置（１１０，５２０）または前記もう１つのデータ記録装置へ送信するとともに前記第４のセッション鍵を前記第３の履歴情報として前記もう１つの履歴情報保持部（１４１５Ａ，７０）に格納し、外部からの履歴情報の出力要求に応じて前記もう１つの通信情報および前記第３の履歴情報を出力する、請求項１０に記載のデータ記録装置。

１２．前記もう１つの通信情報と前記第３の履歴情報とに対する電子署名を生成する電子署名生成部（１４２０）をさらに備え、

前記制御部（１４２０）は、外部からの履歴情報の出力要求に応じて、前記もう１つの通信情報と前記第３の履歴情報と前記電子署名とを出力する、請求項１１に記載のデータ記録装置。

１３．前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から入力された第５のセッション鍵によって暗号化する暗号処理部（１４０６）をさらに備え、

前記制御部（１４２０）は、前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から前記独自データを受信する通信の確立時、前記第４のセッション鍵を前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置に出力するとともに前記第４のセッション鍵を前記第３の履歴情報として前記もう１つの履歴情報保持部（１４１５Ａ，７０）に格納し、外部からの履歴情報の出力要求に応じて前記もう１つの通信情報と前記暗号処理部（１４０６）において前記第５のセッション鍵によって暗号化された前記第３の履歴情報とを出力する、請求項１１に記載のデータ記録装置。

１４．前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から入力された第５のセッション鍵によってデータを暗号化する暗号処理部（１４０６）と、

前記通信情報（７３）と前記暗号処理部（１４０６）において外部から入力さ

れた第３のセッション鍵によって暗号化された第３の履歴情報とに対する電子署名を生成する電子署名生成部（１４２０）とをさらに備え、

前記暗号処理部（１４０６）は、前記第５のセッション鍵によって前記第３の履歴情報と前記電子署名とを暗号化し、

前記制御部（１４２０）は、前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から前記独自データを受信する通信の確立時、前記第４のセッション鍵を前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置に出力するとともに前記第４のセッション鍵を前記第３の履歴情報として前記もう１つの履歴情報保持部（１４１５Ａ，７０）に格納し、外部からの履歴情報の出力要求に応じて、前記通信情報（７３）と前記第５のセッション鍵によって暗号化された前記第３の履歴情報と前記第５のセッション鍵によって暗号化された前記電子署名とを出力する、請求項１１に記載のデータ記録装置。

１５．前記制御部（１４２０）は、前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの移動の対象となる独自データを特定する第３のデータ特定情報を前記通信情報保持部（１４１５Ａ，７０）に記録し、前記第３のデータ特定情報の出力要求に応じて、前記通信情報保持部（１４１５Ａ，７０）から前記第３のデータ特定情報を読出して前記通信情報（７３）および前記第３の履歴情報とともに出力する、請求項１０に記載のデータ記録装置。

１６．前記独自データは、暗号化コンテンツデータを復号するためのライセンスである、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

補正書の請求の範囲

［２００２年７月３日（０３．０７．０２）国際事務局受理：出願当初の請求の範囲５、８、９及び１０－１６は補正された；新しい請求の範囲１７が加えられた；他の請求の範囲は変更なし。（８頁）］

３．前記履歴情報保持部（１４１５Ａ，８０）は、前記移動の対象となった独自データを外部へ出力不可能な状態でさらに保持し、

前記制御部（１４２０）は、

前記独自データの前記他のデータ記録装置（１１０，５２０）への移動に対して前記移動の対象となった独自データを前記履歴情報保持部（１４１５Ａ，８０）に与え、前記独自データ保持部から前記移動の対象となった独自データを消去し、

前記独自データの復元時、前記履歴情報保持部（１４１５Ａ，８０）に保持された独自データを前記独自データ保持部に書込む、請求項１に記載のデータ記録装置。

４．前記第１の履歴情報（８１）は、前記移動のための通信確立時に前記他のデータ記録装置（１１０，５２０）で生成され、かつ、前記他のデータ記録装置（１１０，５２０）から受信された第１のセッション鍵であり、

前記第２の履歴情報（７２）は、前記移動のための通信確立時に前記他のデータ記録装置（１１０，５２０）で生成され、かつ、前記他のデータ記録装置（１１０，５２０）に保持された前記第１のセッション鍵と同じ第２のセッション鍵である、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

５．（補正後）電子署名により前記通信情報（７３）と前記第２の履歴情報（７２）との正当性を確認する署名確認部（１４２０）をさらに備え、

前記制御部（１４２０）は、さらに、前記通信情報（７３）と前記第２の履歴情報（７２）とに対する電子署名を前記通信情報（７３）および前記第２の履歴情報（７２）とともに前記他のデータ記録装置（１１０，５２０）から受信し、前記署名確認部（１４２０）によって前記通信情報（７３）と前記第２の履歴情報（７２）の正当性が確認されたとき、前記通信状態を確認し、かつ、前記第１の履歴情報（８１）と前記第２の履歴情報（７２）との一致を確認する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

６．前記他のデータ記録装置（１１０，５２０）との通信を特定するためのセッション鍵を生成するセッション鍵生成部（１４１８）と、

前記セッション鍵生成部（ｉ４１８）が生成したセッション鍵によって暗号化

されたデータを復号する復号部（１４１２）とをさらに備え、

前記独自データの復元時、

前記セッション鍵生成部（１４１８）は、前記独自データの復元のための通信を特定する第３のセッション鍵を生成し、

前記制御部（１４２０）は、前記第３のセッション鍵を前記他のデータ記録装置（１１０，５２０）へ送信し、前記第３のセッション鍵によって暗号化された第２の履歴情報（７２）を前記他のデータ記録装置（１１０，５２０）から受信する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

７．前記他のデータ記録装置（１１０，５２０）との通信を特定するためのセッション鍵を生成するセッション鍵生成部（１４１８）と、

前記セッション鍵生成部（１４１８）が生成したセッション鍵によって暗号化されたデータを復号する復号部（１４１２）とをさらに備え、

前記独自データの復元時、

前記セッション鍵生成部（１４１８）は、前記独自データの復元のための通信を特定する第３のセッション鍵を生成し、

前記制御部（１４２０）は、前記第３のセッション鍵を前記他のデータ記録装置（１１０，５２０）へ送信し、前記第３のセッション鍵によって暗号化された第２の履歴情報（７２）と、前記第３のセッション鍵によって暗号化された前記電子署名のデータとを前記他のデータ記録装置（１１０，５２０）から受信する、請求項５に記載のデータ記録装置。

８．（補正後）前記履歴情報保持部（１４１５Ａ，８０）は、前記移動の対象となった独自データに含まれる第１のデータ特定情報を前記第１の履歴情報（８１）とともに保持し、

前記制御部（１４２０）は、さらに、前記他のデータ記録装置（１１０，５２０）から受信する前記移動の対象となった第２のデータ特定情報が前記第１のデータ特定情報に一致するか否かを判定し、前記第２のデータ特定情報が前記第１のデータ特定情報に一致するとき、前記通信情報（７３）を確認し、かつ、前記第１の履歴情報（８１）と前記第２の履歴情報（７２）との一致を確認する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

９．（補正後）電子署名により前記通信情報（７３）と前記第２の履歴情報（７２）と前記第２のデータ特定情報との正当性を確認する署名確認部（１４２０）をさらに備え、

前記制御部（１４２０）は、さらに、前記通信情報（７３）と前記第２の履歴情報（７２）と前記第２のデータ特定情報とに対する電子署名を、前記通信情報（７３）と前記第２の履歴情報（７２）と前記第２のデータ特定情報とともに受信し、前記署名確認部（１４２０）によって前記通信情報（７３）と前記第２の履歴情報（７２）と前記第２のデータ特定情報の正当性が確認されたとき、前記第２のデータ特定情報と前記第１のデータ特定情報との一致を確認し、かつ、前記通信情報（７３）を確認し、前記第１の履歴情報（８１）と前記第２の履歴情報（７２）との一致を確認する、請求項８に記載のデータ記録装置。

１０．（補正後）前記他のデータ記録装置（１１０，５２０）または前記他のデータ記録装置（１１０，５２０）と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報（７３）を保持する通信情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴情報保持部（１４１５Ａ，７０）とをさらに備え、

前記制御部（１４２０）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報保持部（１４１５Ａ，７０）に保持されるもう１つの通信情報を更新し、前記第３の履歴情報を前記もう１つの履歴情報保持部（１４１５Ａ，７０）に記録し、外部からの履歴情報の出力要求に応じて前記もう１つの通信情報（７３）と前記第３の履歴情報とを出力する、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

１１．（補正後）前記他のデータ記録装置（１１０，５２０）または前記他のデータ記録装置（１１０，５２０）と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報（７３）を保持する通信情報保持部（１４１５

Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置との通信を特定するためのセッション鍵を生成するセッション鍵生成部（１４１８）をさらに備え、

前記移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つのデータ記録装置から受信する通信の確立時、

前記セッション鍵生成部（１４１８）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するための通信を特定する第４のセッション鍵を生成し、

前記制御部（１４２０）は、前記第４のセッション鍵を前記他のデータ記録装置（１１０，５２０）または前記もう１つのデータ記録装置へ送信するとともに前記第４のセッション鍵を前記第３の履歴情報として前記もう１つの履歴情報保持部（１４１５Ａ，７０）に格納し、受信する通信の進行と共に前記通信情報保持部（１４１５Ａ，７０）に保持されるもう１つの通信情報を更新し、外部からの履歴情報の出力要求に応じて前記もう１つの通信情報（７３）および前記第３の履歴情報を出力する、請求項４に記載のデータ記録装置。

１２．（補正後）前記他のデータ記録装置（１１０，５２０）または前記他のデータ記録装置（１１０，５２０）と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報（７３）を保持する通信情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴情報保持部（１４１５Ａ，７０）と、

前記もう１つの通信情報と前記第３の履歴情報とに対する電子署名を生成する電子署名生成部（１４２０）をさらに備え、

前記制御部（１４２０）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報部（１４１５Ａ，７０）に保持されるもう１つの通信情報を更新し、前記第３の履歴情報を前記もう１つの履歴情報保持部（１４１５Ａ，７０）に記録し、外部からの履歴情報の出力要求に応じて、前記もう１つの通信情報と前記第３の履歴情報と前記電子署名とを出力する、請求項５に記載のデータ記録装置。

１３．（補正後）前記他のデータ記録装置（１１０，５２０）または前記他のデータ記録装置（１１０，５２０）と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報（７３）を保持する通信情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から入力された第４のセッション鍵によって暗号化する暗号処理部（１４０６）をさらに備え、

前記制御部（１４２０）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報保持部（１４１５Ａ，７０）に保持されるもう１つの通信情報を更新し、前記第３の履歴情報を前記もう１つの履歴情報保持部（１４１５Ａ，７０）に記録し、外部からの履歴情報の出力要求に応じて前記もう１つの通信情報と前記暗号処理部（１４０６）において前記第４のセッション鍵によって暗号化された前記第３の履歴情報とを出力する、請求項６に記載のデータ記録装置。

１４．（補正後）前記他のデータ記録装置（１１０，５２０）または前記他のデータ記録装置（１１０，５２０）と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報（７３）を保持する通信情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から入力された第４のセッション鍵によってデータを暗号化する暗号処理部（１４０６）と、

前記もう１つの通信情報（７３）と前記暗号処理部（１４０６）において外部から入力された第４のセッション鍵によって暗号化された第３の履歴情報とに対する電子署名を生成する電子署名生成部（１４２０）とをさらに備え、

前記暗号処理部（１４０６）は、前記第４のセッション鍵によって前記第３の履歴情報と前記電子署名とを個々に暗号化し、

前記制御部（１４２０）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報保持部（１４１５Ａ，７０）に保持されるもう１つの通信情報を更新し、前記第３の履歴情報を前記もう１つの履歴情報保持部（１４１５Ａ，７０）に記録し、外部からの履歴情報の出力要求に応じて、前記もう１つの通信情報（７３）と前記第４のセッション鍵によって暗号化された前記第３の履歴情報と前記第４のセッション鍵によって暗号化された前記電子署名とを出力する、請求項７に記載のデータ記録装置。

１５．（補正後）前記他のデータ記録装置（１１０，５２０）または前記他のデータ記録装置（１１０，５２０）と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報（７３）と前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの移動の対象となる独自データを特定する第３のデータ特定情報とを保持する通信情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴情報保持部（１４１５Ａ，７０）と、

前記もう１つの通信情報と前記第３の履歴情報と前記第３のデータ特定情報とに対する電子署名を生成する電子署名生成部（１４２０）とをさらに備え、

前記制御部（１４２０）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報保持部（１４１５Ａ，７０）に保持されるもう１つの通信情報を更新し、前記第３の履歴情報と前記第３のデータ特定情報とを前記通信情報部（１４１５Ａ，７０）に記録し、外部からの履歴情報の出力要求に応じて、前記通信情報保持部（１４１５Ａ，７０）に記録された前記第３のデータ特定情報と前記もう１つの通信情報（７３）および前記もう１つの履歴情報保持部（１４１５Ａ，７０）に保持された前記第３の履歴情報と、前記電子署名生成部によって生成された電子署名とを出力する、請求項８に記載のデータ記録装置。

１６．（補正後）前記他のデータ記録装置（１１０，５２０）または前記他のデータ記録装置（１１０，５２０）と異なるもう１つの他のデータ記録装置との通信状態を示すもう１つの通信情報（７３）と前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの移動の対象となる独自データを特定する第３のデータ特定情報とを保持する通信情報保持部（１４１５Ａ，７０）と、

前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置からの独自データの移動処理を特定するための第３の履歴情報を保持するもう１つの履歴情報保持部（１４１５Ａ，７０）とをさらに備え、

前記制御部（１４２０）は、前記独自データの移動処理において移動対象となる独自データを前記他のデータ記録装置（１１０，５２０）または前記もう１つの他のデータ記録装置から受信するとき、受信する通信の進行と共に前記通信情報保持部（１４１５Ａ，７０）に保持されるもう１つの通信情報を更新し、前記第３の履歴情報と前記第３のデータ特定情報とを前記通信情報保持部（１４１５Ａ，７０）に記録し、外部からの履歴情報の出力要求に応じて、前記通信情報保持部（１４１５Ａ，７０）に記録されている前記第３のデータ特定情報と前記もう１つの通信情報（７３）および前記もう１つの履歴情報保持部（１４１５Ａ，

７０）に保持された前記第３の履歴情報とを出力する、請求項９に記載のデータ記録装置。

１７．（追加）前記暗号化コンテンツデータを記憶する記憶部をさらに備え、

前記独自データは、暗号化コンテンツデータを復号するためのライセンスである、請求項１から請求項３のいずれか１項に記載のデータ記録装置。

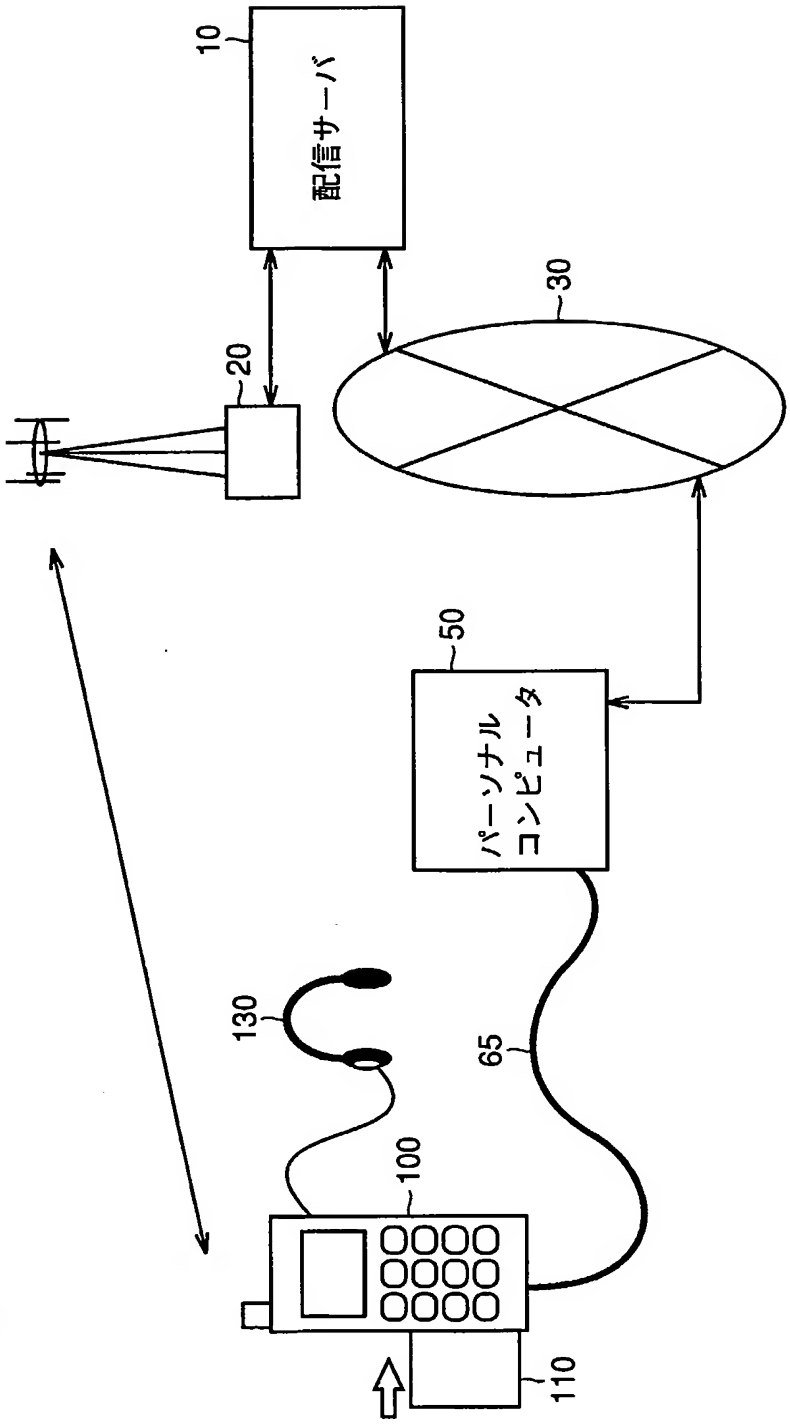


FIG.1

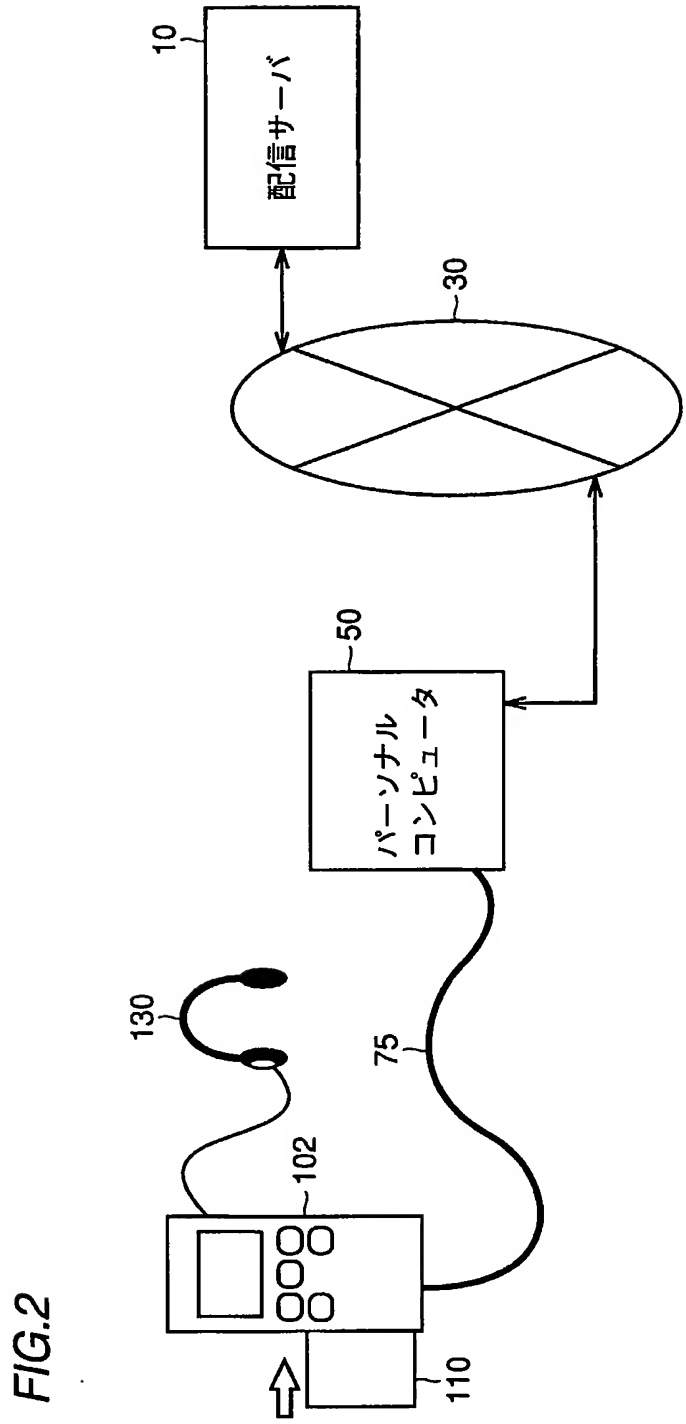


FIG.2

FIG.3

記号	種類	属性	特性
Dc	コンテンツデータ	コンテンツ固有	例：音楽データ、朗読データ、教材データ、画像データ Kcにて復号可能な暗号化コンテンツデータ {Dc}Kcとして配信され、メモリカードに保持される
Dc-inf	付加情報	コンテンツ固有	Dcに付随する平文データ。
Kc	ライセンス	コンテンツ固有	ライセンス 暗号化コンテンツデータを復号する復号鍵
ACm/ACp	ライセンス	ライセンス固有	制限情報 再生やライセンスの取り扱いに対する制限事項
コンテンツID	ライセンス	コンテンツ固有	コンテンツを特定するための管理コード
ライセンスID	ライセンス	ライセンス固有	ライセンスを特定するための管理コード
ライセンス	ライセンス	ライセンス固有	Kc+ACm+ACp+コンテンツID+ライセンスIDの総称
有効フラグ	フラグ	ライセンス固有	ライセンスをメモリーカードから外部へ出すことが可能か否かを表す。

FIG.4

	記号	種類	属性	特性
配信サーバ	KPa/KPb	公開認証鍵	システム共通	認証局にて認証データを復号する鍵 KPaはレベル1、KPbはレベル2
	Ks1	共通鍵	セッション固有	メモリカード、ライセンス専用メモリーカードへのライセンス配信ごとに発生
メモリカード ライセンス専用メモリーカード	KPa	公開認証鍵	システム共通	認証局にて認証データを復号する鍵 配信サーバのKPaと同一
	KPmw	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 wはクラスを識別するための識別子
	Kmw	秘密復号鍵	クラス固有	公開暗号鍵KPmwにて暗号化されたデータを復号する非対称な復号鍵
	KPmcx	公開暗号鍵	個別	メモリカードごとに異なる。 xはモジュールを識別するための識別子
	Kmcx	秘密復号鍵	個別	公開暗号鍵KPmcxにて暗号化されたデータを復号する非対称な復号鍵
	Ks2	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間のライセンスの授受ごとに発生
	Cmw	証明書	クラス証明書	メモリカード、ライセンス専用メモリーカードのクラス証明書。 認証機能を有する。 {KPmw//Cmw}KPaの形式で出荷時に記録。 ＊メモリカード、ライセンス管理デバイス、およびライセンス管理モジュールのクラスwごとに異なる。
コンテンツ再生回路	KPpy	公開暗号鍵	クラス固有	証明書Cmwとともに認証局にて暗号化された認証データとして保持 yはクラスを識別するための識別子
	Kpy	秘密復号鍵	クラス固有	公開暗号鍵KPpyにて暗号化されたデータを復号する非対称な復号鍵
	Ks3	共通鍵	セッション固有	配信サーバまたは音楽再生モジュール間の再生セッションごとに発生
	Cpy	証明書	クラス証明書	コンテンツ再生回路のクラス証明書。認証機能を有する。 {KPpy//Cpy}KPaの形式で出荷時に記録。 ＊コンテンツ再生回路のクラスyごとに異なる。

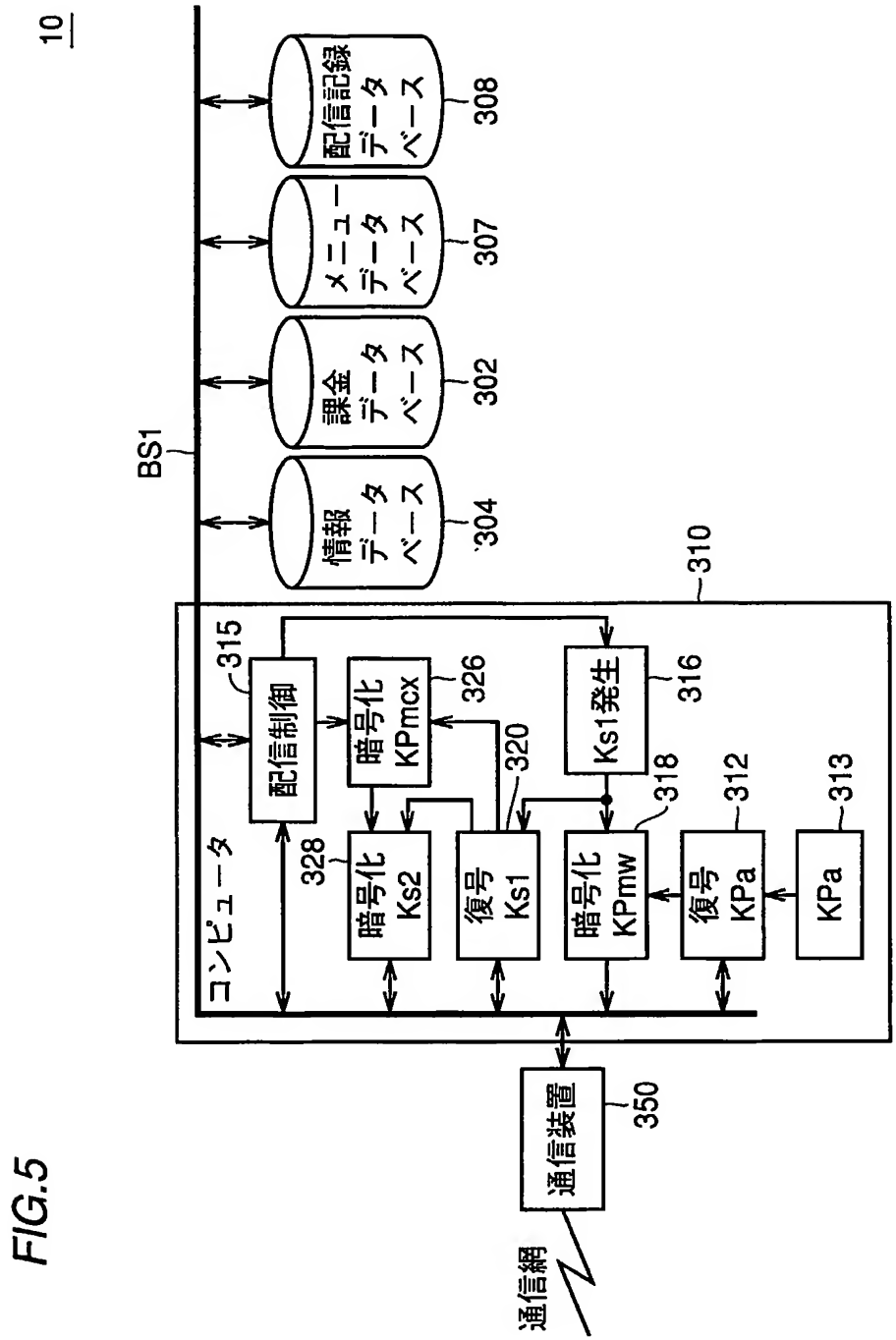

10
BS1
情報データベース
304
課金データベース
302
メニューデータベース
307
配信記録データベース
308
310
コンピュータ
315
配信制御
暗号化 KPmcx
326
320
Ks1発生
316
318
328
暗号化 Ks2
復号 Ks1
暗号化 KPmw
312
復号 KPa
313
KPa
通信装置
350
通信網

FIG.5

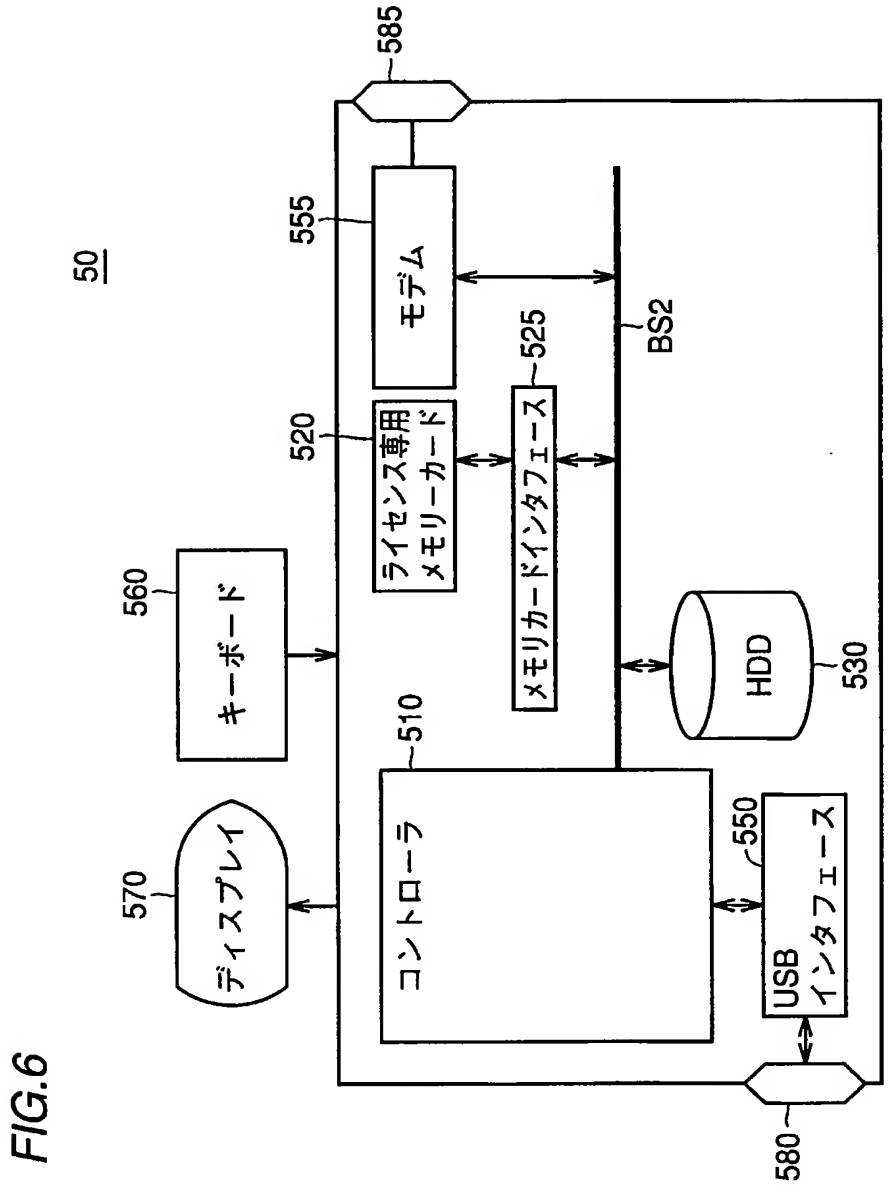
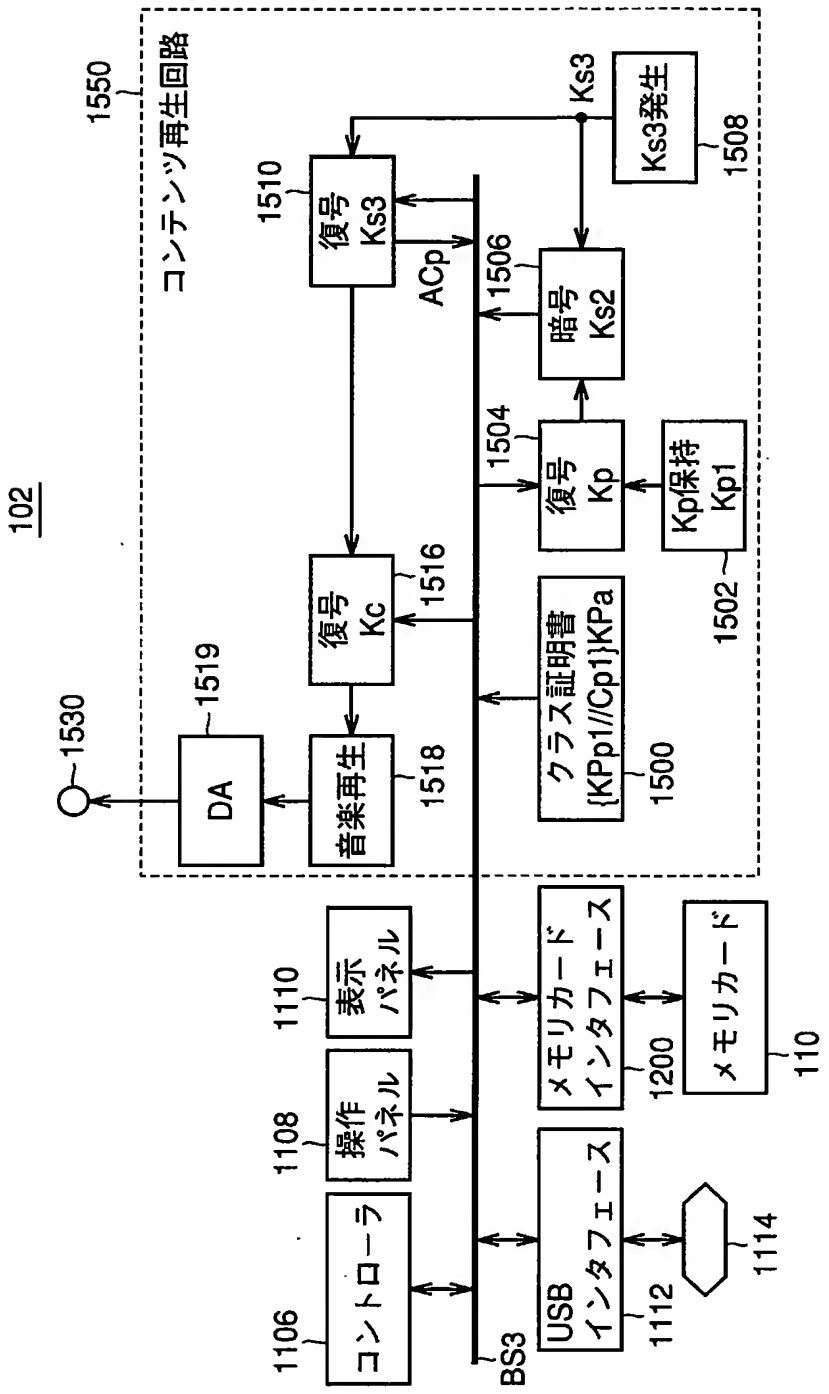

50
585
555
モデム
BS2
525
520
ライセンス専用
メモリーカード
メモリカードインタフェース
560
キーボード
HDD
530
510
コントローラ
570
ディスプレイ
550
USB
インタフェース
580

FIG.6

FIG.7


102
1550
コンテンツ再生回路
1530
1519
DA
1518
音楽再生
1516
復号 Kc
1510
復号 Ks3
ACp
1506
暗号 Ks2
Ks3
Ks3発生
1508
1504
復号 Kp
Kp保持 Kp1
1502
クラス証明書 {KPp1//Cp1}KPa
1500
1110
表示パネル
1108
操作パネル
1106
コントローラ
BS3
メモリカードインタフェース
1200
メモリカード
110
USB インタフェース
1112
1114

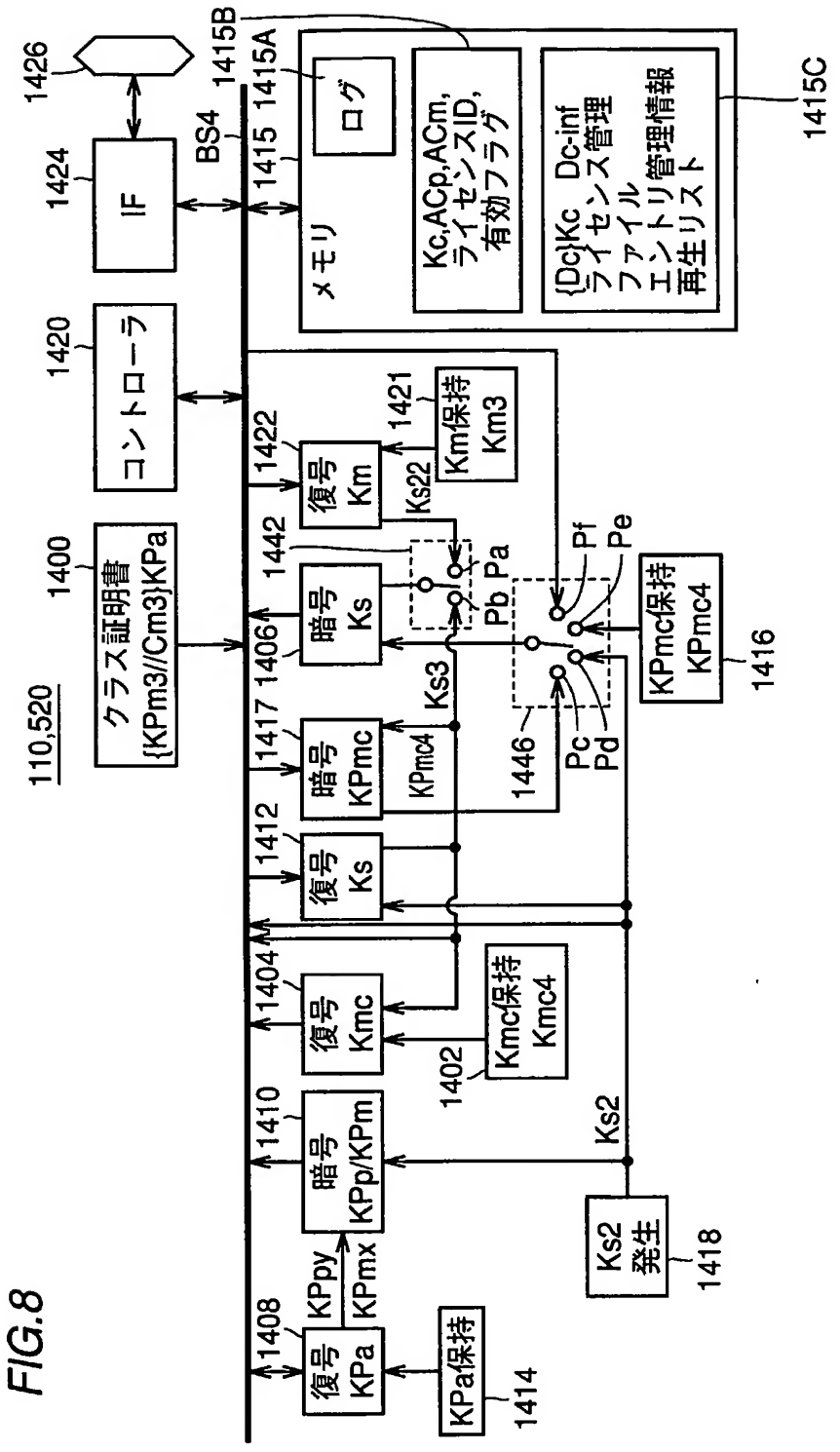

1426
1424
IF
BS4
1415
1415B
1415A
ログ
メモリ
Kc,ACp,ACm,
ライセンスID,
有効フラグ
{Dc}Kc Dc-inf
ライセンス管理
ファイル
エントリ管理情報
再生リスト
1415C
1420
コントローラ
1400
クラス証明書
{KPm3//Cm3}KPa
110,520
1422
復号
Km
1421
Km保持
Km3
Ks22
1442
暗号
Ks
Pb Pa
Pf
Pe
1406
Ks3
1417
暗号
KPmc
KPmc4
1446
Pc
Pd
KPmc保持
KPmc4
1416
1412
復号
Ks
1404
復号
Kmc
Kmc保持
Kmc4
1402
1410
暗号
KPp/KPm
Ks2
KPpy
KPmx
Ks2
発生
1418
1408
復号
KPa
KPa保持
1414

FIG.8

FIG.9

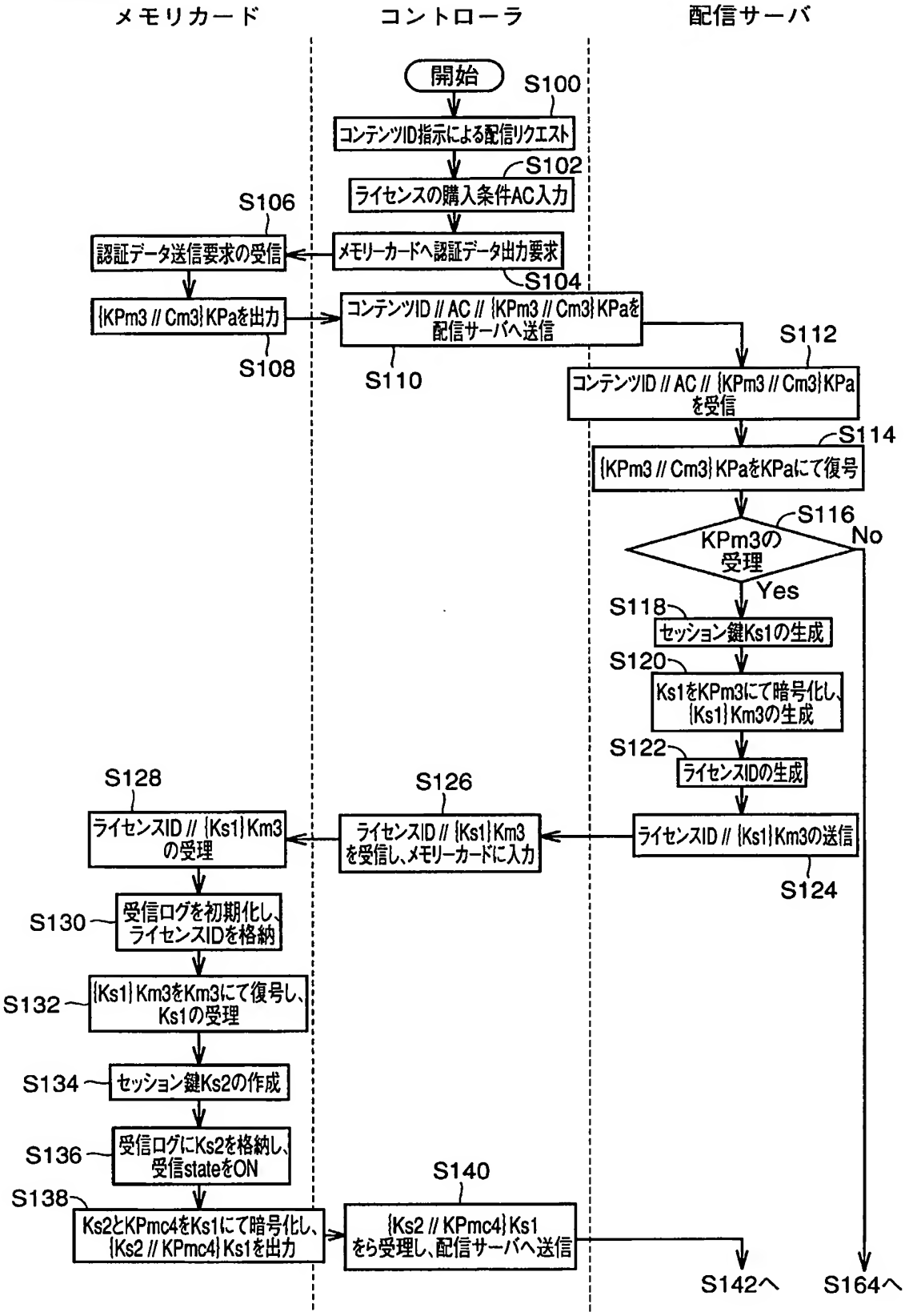

メモリカード
コントローラ
配信サーバ
開始
S100
コンテンツID指示による配信リクエスト
S102
ライセンスの購入条件AC入力
S106
認証データ送信要求の受信
メモリーカードへ認証データ出力要求
S104
{KPm3 // Cm3}KPaを出力
コンテンツID // AC // {KPm3 // Cm3}KPaを配信サーバへ送信
S108
S110
S112
コンテンツID // AC // {KPm3 // Cm3}KPaを受信
S114
{KPm3 // Cm3}KPaをKPaにて復号
S116
KPm3の受理
No
Yes
S118
セッション鍵Ks1の生成
S120
Ks1をKPm3にて暗号化し、{Ks1}Km3の生成
S122
ライセンスIDの生成
S128
S126
ライセンスID // {Ks1}Km3の受理
ライセンスID // {Ks1}Km3を受信し、メモリーカードに入力
ライセンスID // {Ks1}Km3の送信
S124
S130
受信ログを初期化し、ライセンスIDを格納
S132
{Ks1}Km3をKm3にて復号し、Ks1の受理
S134
セッション鍵Ks2の作成
S136
受信ログにKs2を格納し、受信stateをON
S138
S140
Ks2とKPmc4をKs1にて暗号化し、{Ks2 // KPmc4}Ks1を出力
{Ks2 // KPmc4}Ks1をら受理し、配信サーバへ送信
S142へ
S164へ

FIG.10

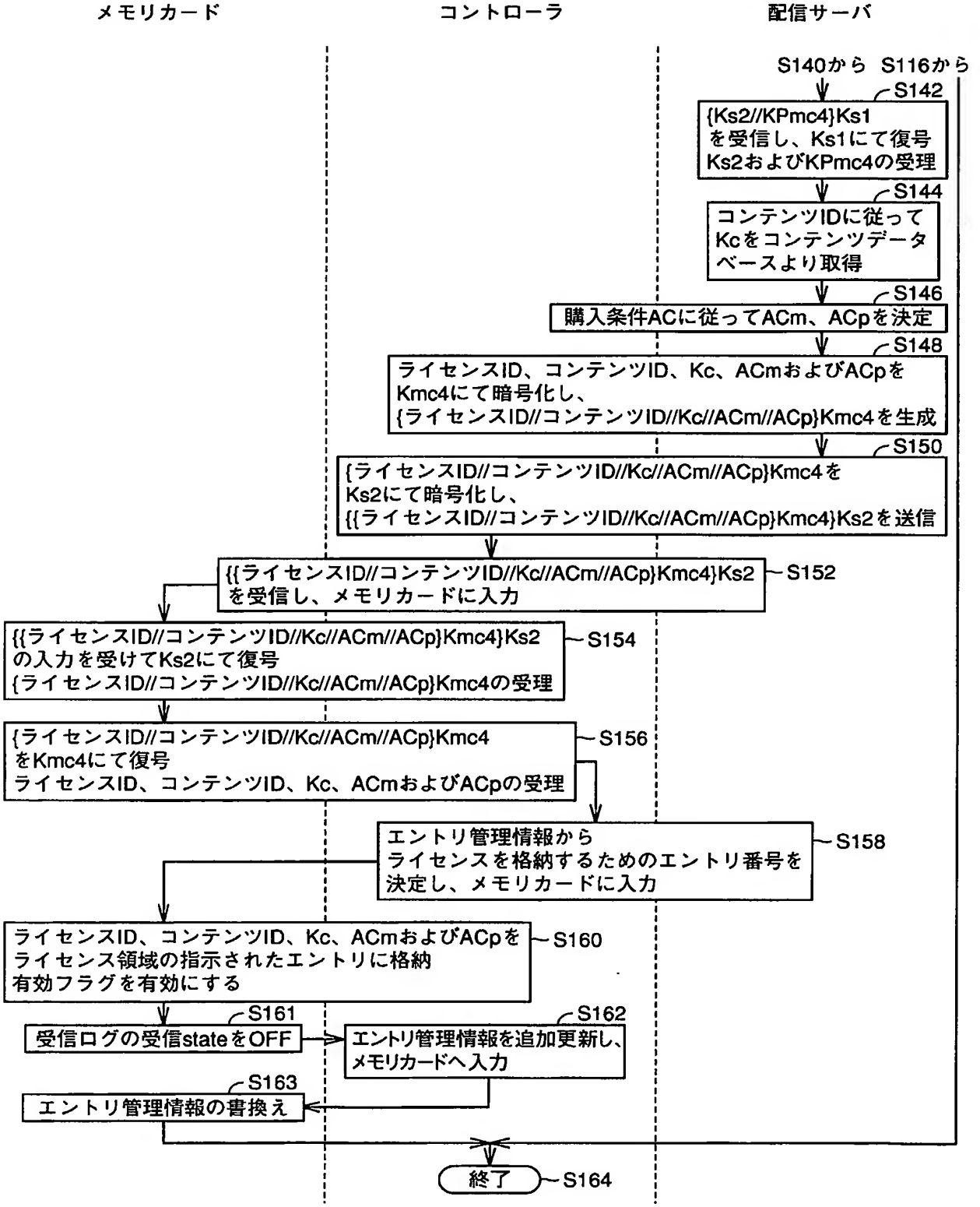

メモリカード
コントローラ
配信サーバ
S140から
S116から
S142
{Ks2//KPmc4}Ks1
を受信し、Ks1にて復号
Ks2およびKPmc4の受理
S144
コンテンツIDに従って
Kcをコンテンツデータ
ベースより取得
S146
購入条件ACに従ってACm、ACpを決定
S148
ライセンスID、コンテンツID、Kc、ACmおよびACpを
Kmc4にて暗号化し、
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を生成
S150
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を
Ks2にて暗号化し、
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2を送信
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2
を受信し、メモリカードに入力
S152
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2
の入力を受けてKs2にて復号
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4の受理
S154
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4
をKmc4にて復号
ライセンスID、コンテンツID、Kc、ACmおよびACpの受理
S156
エントリ管理情報から
ライセンスを格納するためのエントリ番号を
決定し、メモリカードに入力
S158
ライセンスID、コンテンツID、Kc、ACmおよびACpを
ライセンス領域の指示されたエントリに格納
有効フラグを有効にする
S160
受信ログの受信stateをOFF
S161
エントリ管理情報を追加更新し、
メモリカードへ入力
S162
エントリ管理情報の書換え
S163
終了
S164

FIG.11

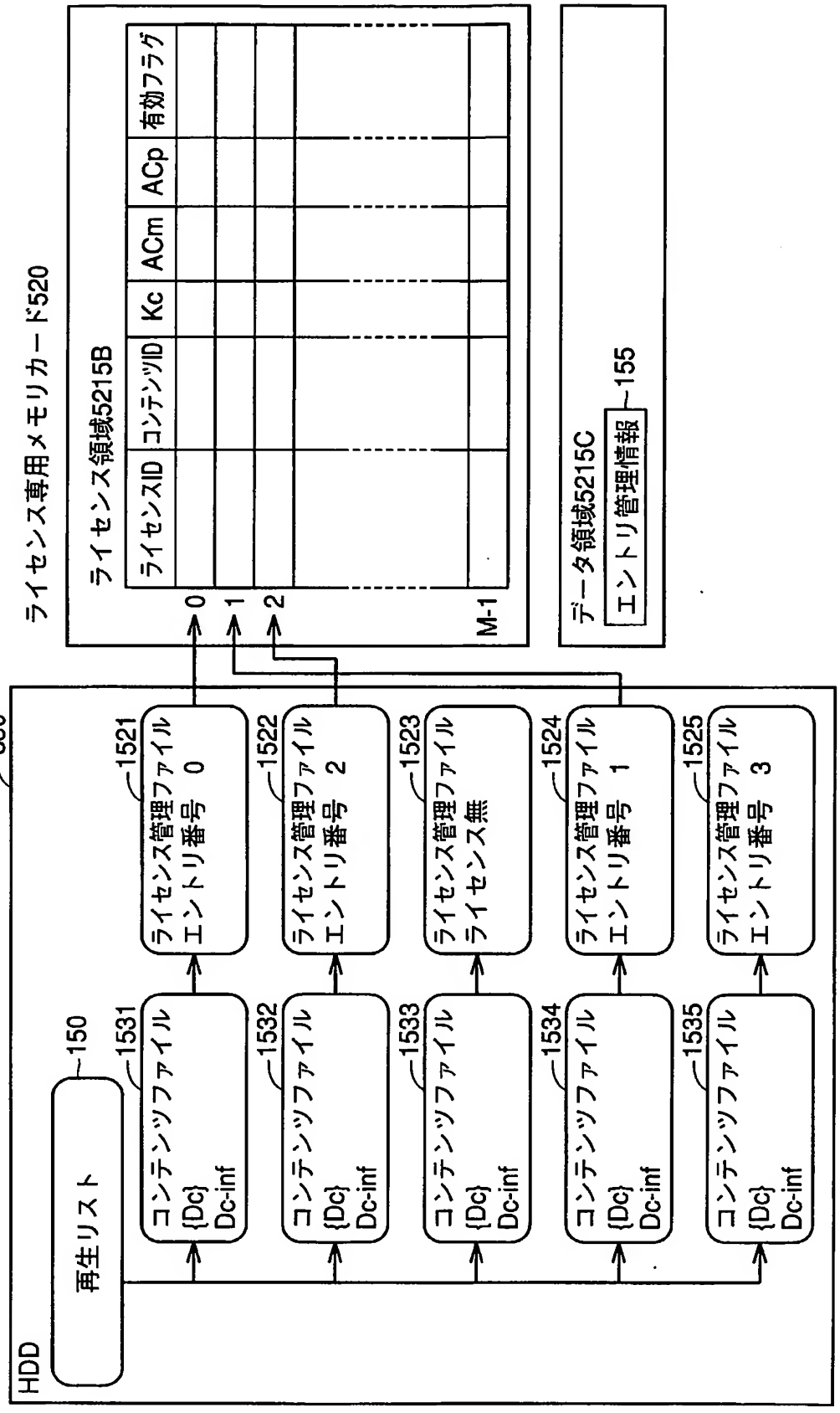

HDD
530
再生リスト
150
コンテンツファイル
{Dc}
Dc-inf
1531
1532
1533
1534
1535
ライセンス管理ファイル
エントリ番号 0
ライセンス管理ファイル
エントリ番号 2
ライセンス管理ファイル
ライセンス無
ライセンス管理ファイル
エントリ番号 1
ライセンス管理ファイル
エントリ番号 3
1521
1522
1523
1524
1525
ライセンス専用メモリカード520
ライセンス領域5215B
ライセンスID
コンテンツID
Kc
ACm
ACp
有効フラグ
0
1
2
M-1
データ領域5215C
エントリ管理情報
155

FIG.12

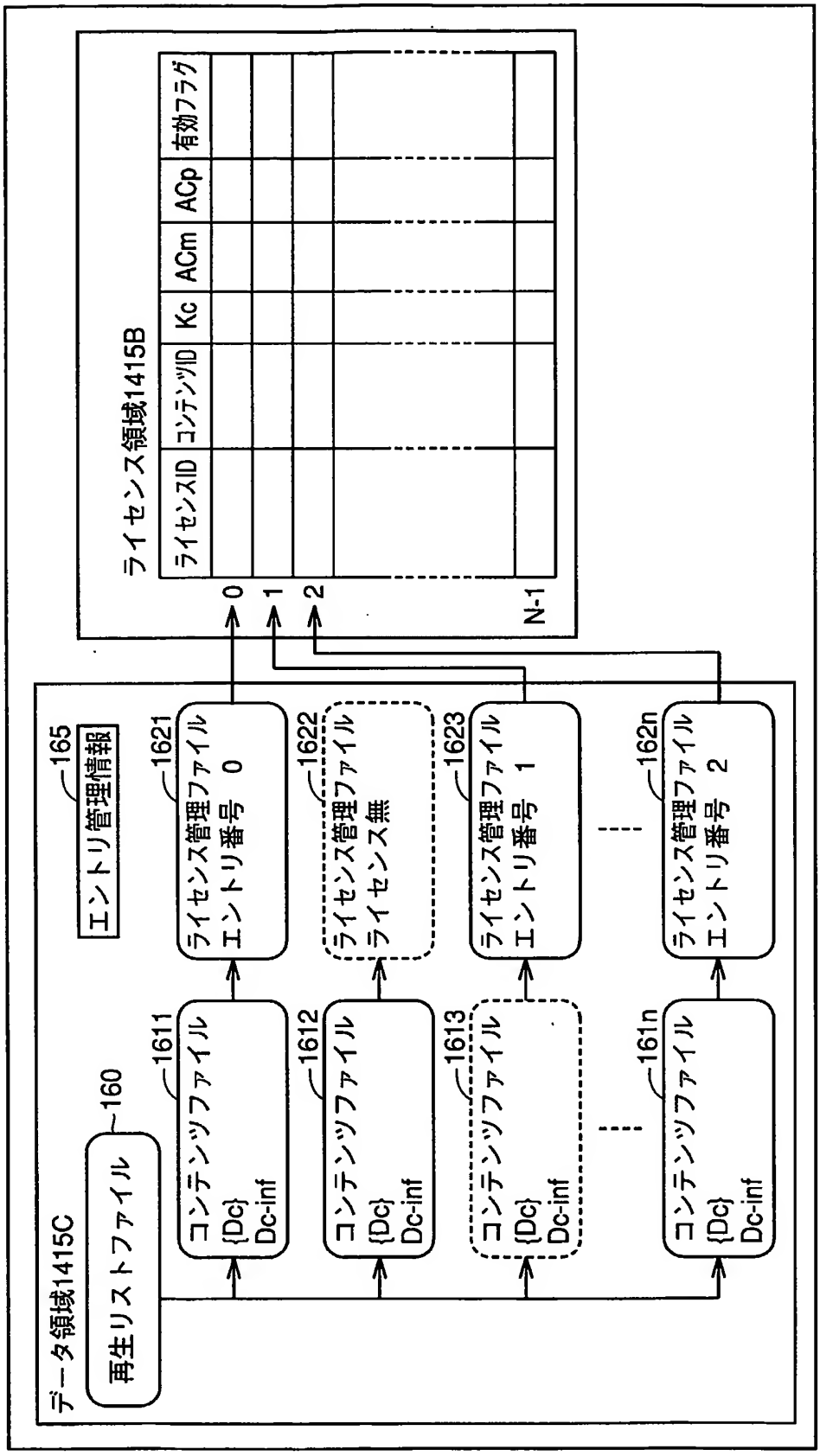

メモリカード110
データ領域1415C
再生リストファイル
160
エントリ管理情報
165
コンテンツファイル {Dc} Dc-inf
1611
コンテンツファイル {Dc} Dc-inf
1612
コンテンツファイル {Dc} Dc-inf
1613
コンテンツファイル {Dc} Dc-inf
161n
ライセンス管理ファイル エントリ番号 0
1621
ライセンス管理ファイル ライセンス無
1622
ライセンス管理ファイル エントリ番号 1
1623
ライセンス管理ファイル エントリ番号 2
162n
ライセンス領域1415B
ライセンスID
コンテンツID
Kc
ACm
ACp
有効フラグ
0
1
2
N-1

FIG.13

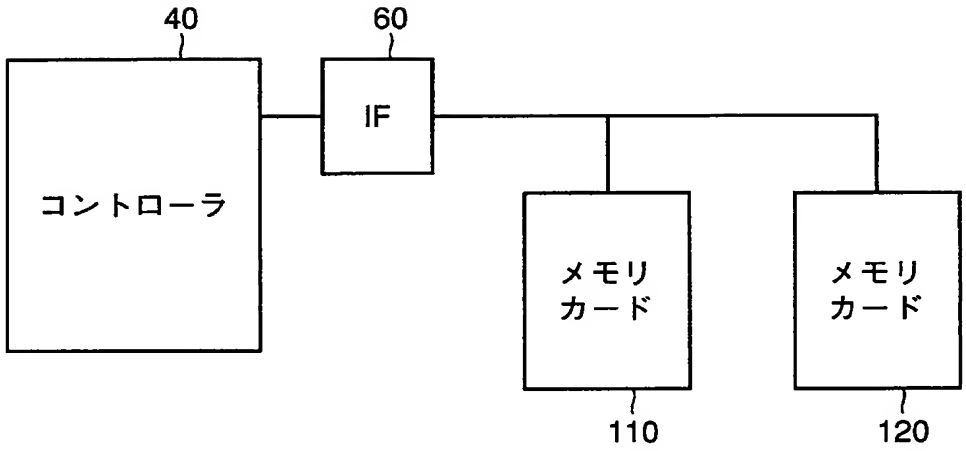


FIG.14

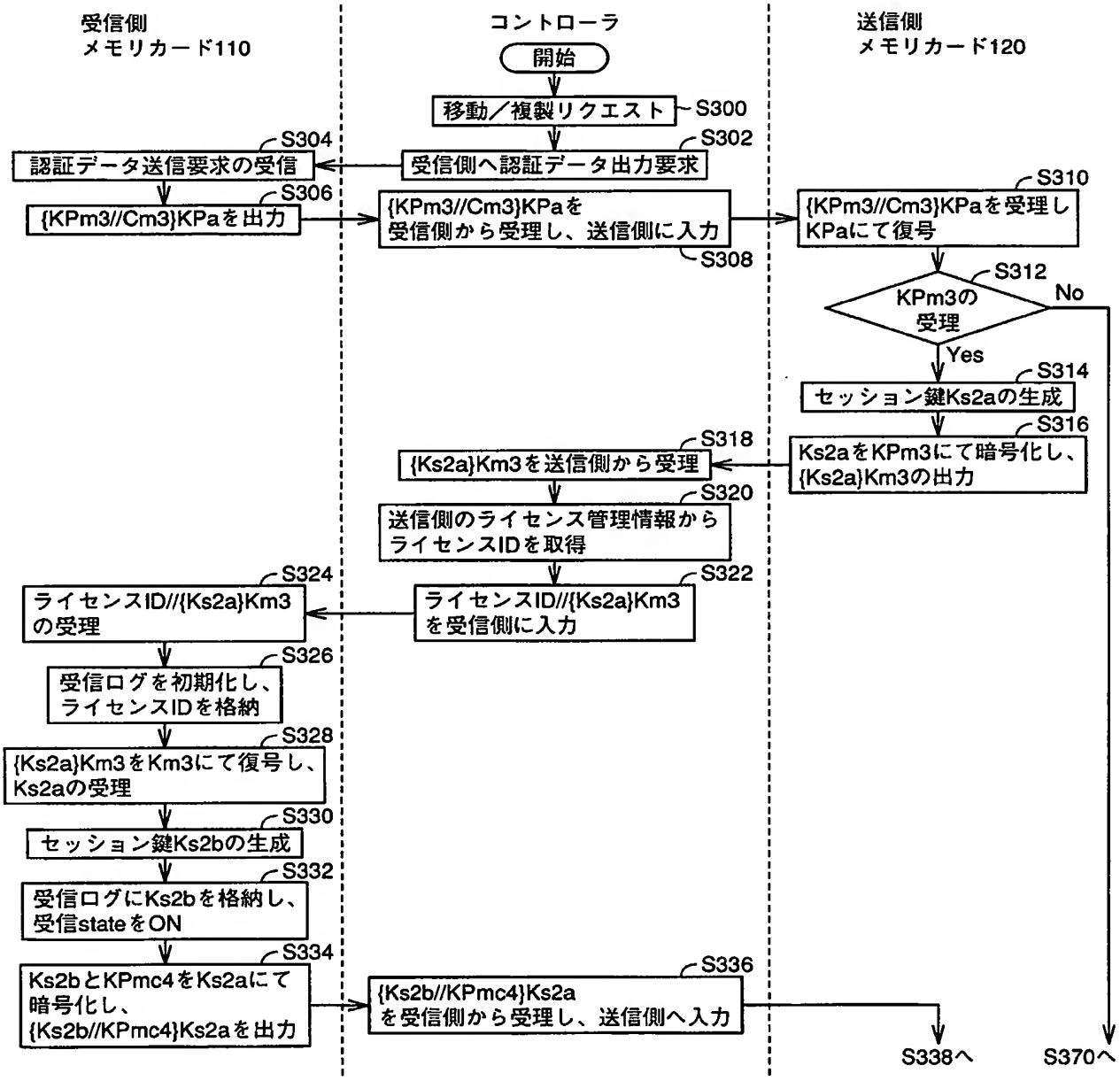

受信側
メモリカード110
コントローラ
送信側
メモリカード120
開始
移動／複製リクエスト
S300
受信側へ認証データ出力要求
S302
認証データ送信要求の受信
S304
{KPm3//Cm3}KPaを出力
S306
{KPm3//Cm3}KPaを
受信側から受理し、送信側に入力
S308
{KPm3//Cm3}KPaを受理し
KPaにて復号
S310
KPm3の
受理
S312
No
Yes
セッション鍵Ks2aの生成
S314
Ks2aをKPm3にて暗号化し、
{Ks2a}Km3の出力
S316
{Ks2a}Km3を送信側から受理
S318
送信側のライセンス管理情報から
ライセンスIDを取得
S320
ライセンスID//{Ks2a}Km3
を受信側に入力
S322
ライセンスID//{Ks2a}Km3
の受理
S324
受信ログを初期化し、
ライセンスIDを格納
S326
{Ks2a}Km3をKm3にて復号し、
Ks2aの受理
S328
セッション鍵Ks2bの生成
S330
受信ログにKs2bを格納し、
受信stateをON
S332
Ks2bとKPmc4をKs2aにて
暗号化し、
{Ks2b//KPmc4}Ks2aを出力
S334
{Ks2b//KPmc4}Ks2a
を受信側から受理し、送信側へ入力
S336
S338へ
S370へ

FIG.15

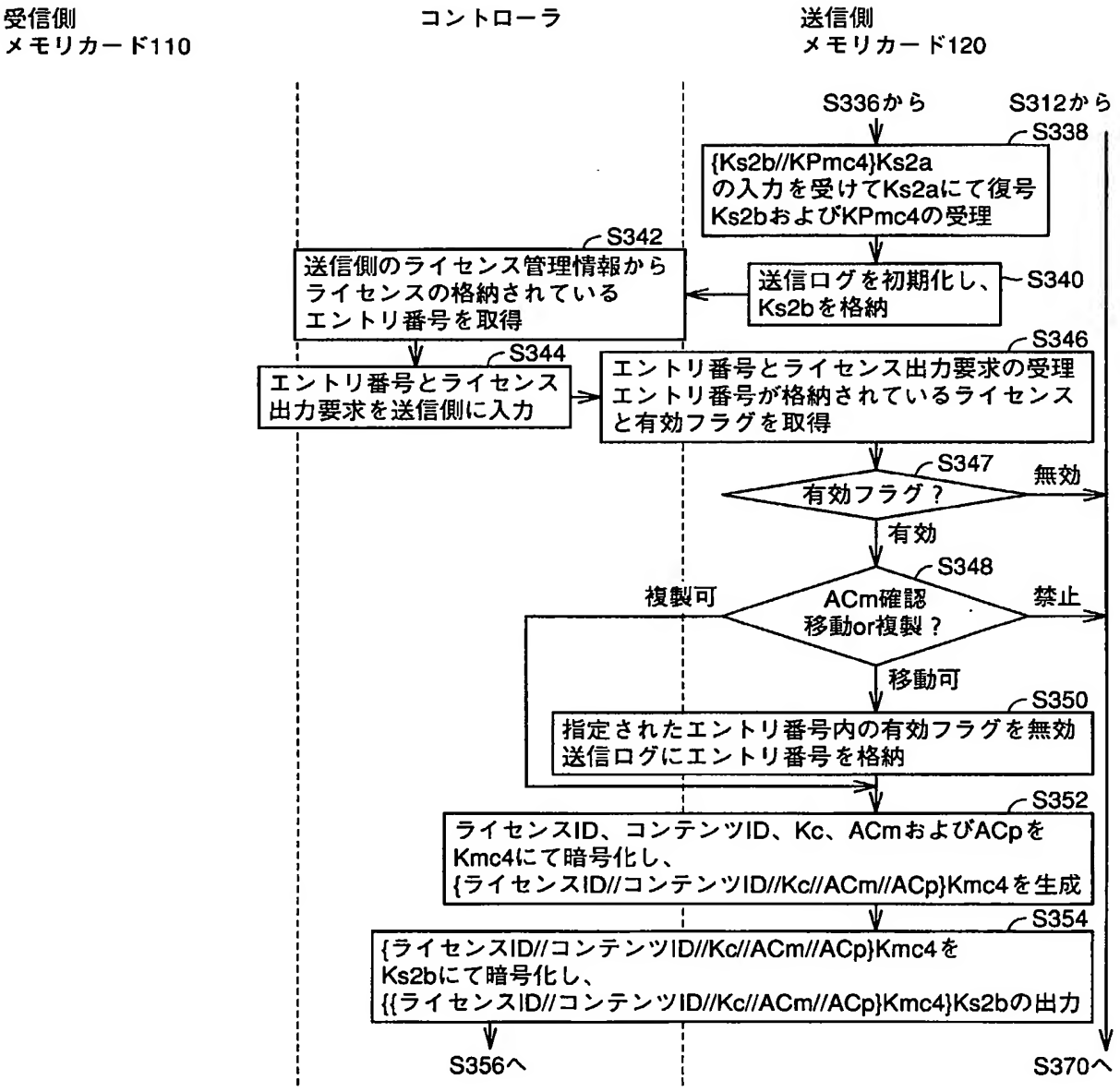

受信側
メモリカード110
コントローラ
送信側
メモリカード120
S336から
S312から
S338
{Ks2b//KPmc4}Ks2a
の入力を受けてKs2aにて復号
Ks2bおよびKPmc4の受理
S342
送信側のライセンス管理情報から
ライセンスの格納されている
エントリ番号を取得
送信ログを初期化し、
Ks2bを格納
S340
S344
エントリ番号とライセンス
出力要求を送信側に入力
S346
エントリ番号とライセンス出力要求の受理
エントリ番号が格納されているライセンス
と有効フラグを取得
S347
有効フラグ？
無効
有効
S348
複製可
ACm確認
移動or複製？
禁止
移動可
S350
指定されたエントリ番号内の有効フラグを無効
送信ログにエントリ番号を格納
S352
ライセンスID、コンテンツID、Kc、ACmおよびACpを
Kmc4にて暗号化し、
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を生成
S354
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4を
Ks2bにて暗号化し、
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2bの出力
S356へ
S370へ

FIG.16

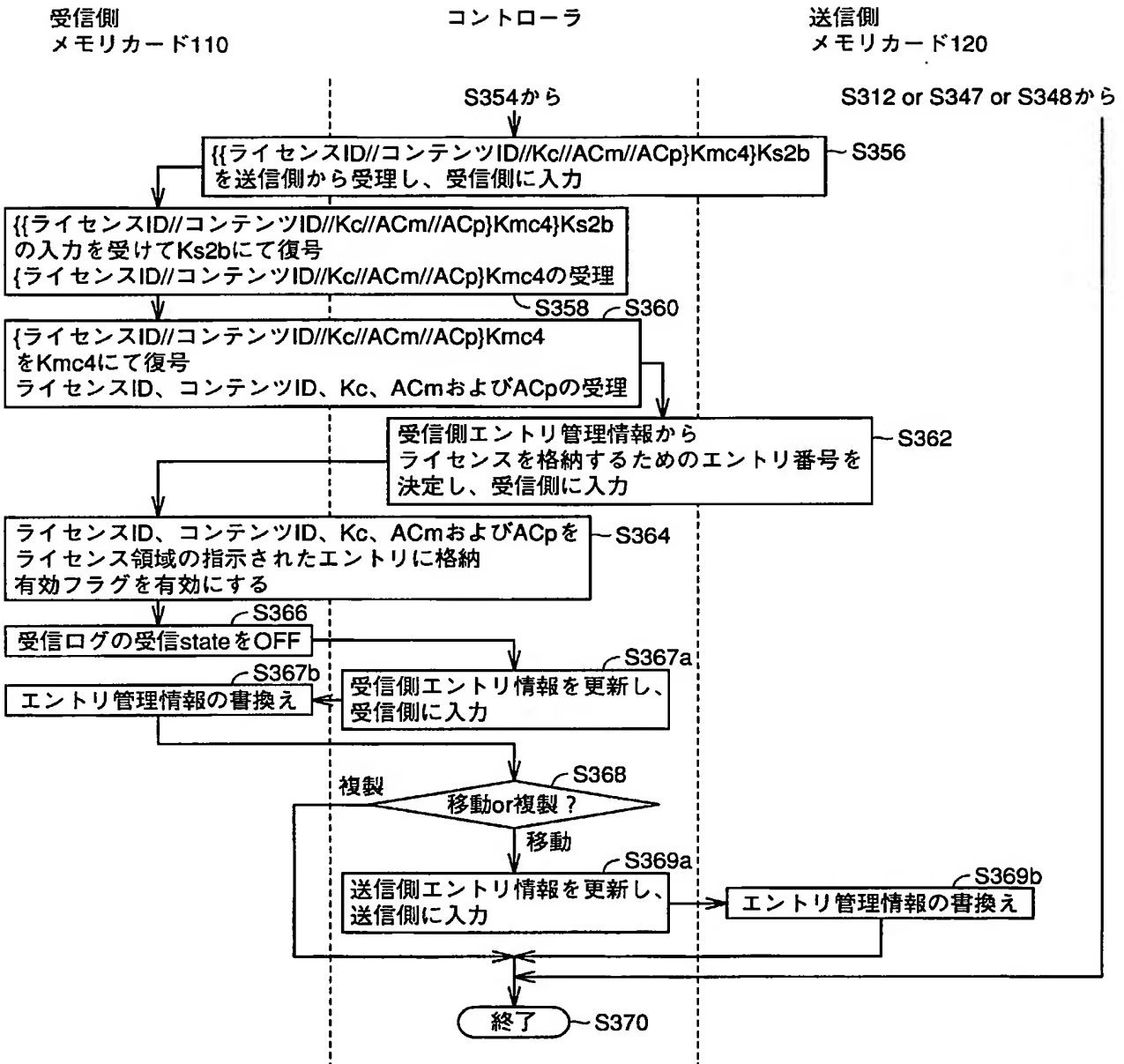

受信側
メモリカード110
コントローラ
送信側
メモリカード120
S354から
S312 or S347 or S348から
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2b
を送信側から受理し、受信側に入力
S356
{{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4}Ks2b
の入力を受けてKs2bにて復号
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4の受理
S358
S360
{ライセンスID//コンテンツID//Kc//ACm//ACp}Kmc4
をKmc4にて復号
ライセンスID、コンテンツID、Kc、ACmおよびACpの受理
受信側エントリ管理情報から
ライセンスを格納するためのエントリ番号を
決定し、受信側に入力
S362
ライセンスID、コンテンツID、Kc、ACmおよびACpを
ライセンス領域の指示されたエントリに格納
有効フラグを有効にする
S364
S366
受信ログの受信stateをOFF
S367a
受信側エントリ情報を更新し、
受信側に入力
S367b
エントリ管理情報の書換え
S368
複製
移動or複製？
移動
S369a
送信側エントリ情報を更新し、
送信側に入力
S369b
エントリ管理情報の書換え
終了
S370

FIG.17

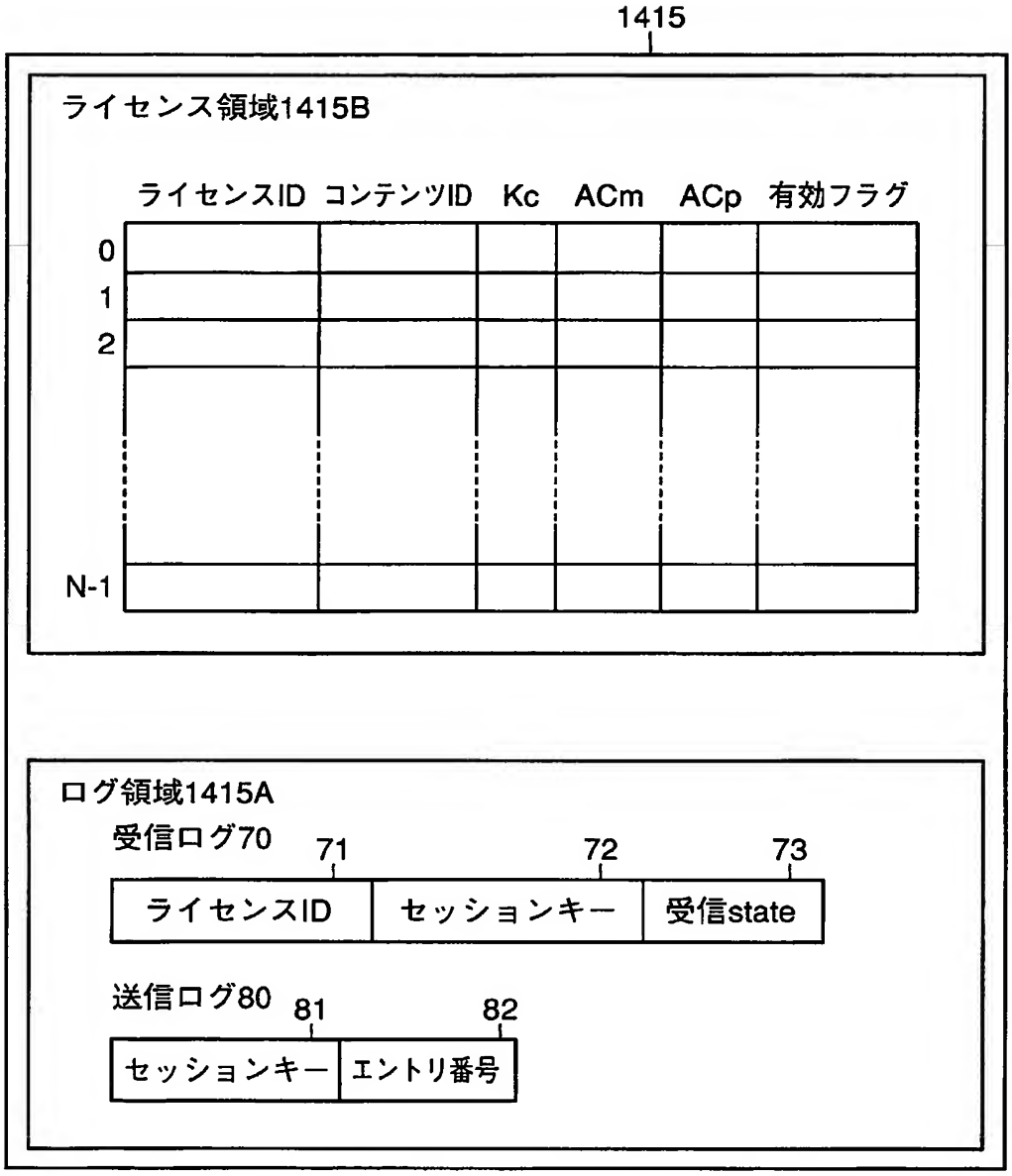

1415
ライセンス領域1415B
ライセンスID
コンテンツID
Kc
ACm
ACp
有効フラグ
0
1
2
N-1
ログ領域1415A
受信ログ70
71
72
73
ライセンスID
セッションキー
受信state
送信ログ80
81
82
セッションキー
エントリ番号

FIG. 18

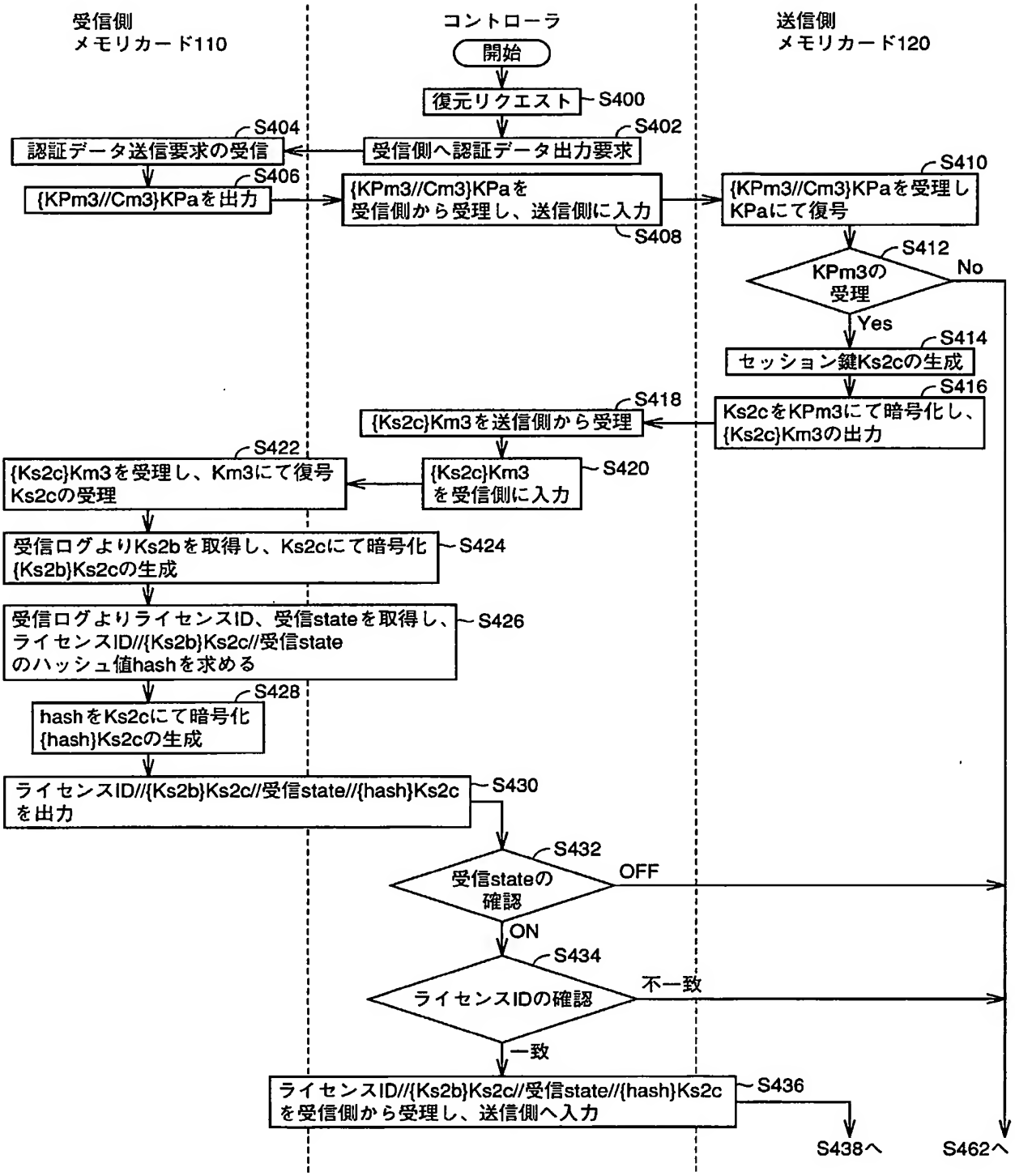

受信側
メモリカード110
コントローラ
送信側
メモリカード120
開始
復元リクエスト
S400
受信側へ認証データ出力要求
S402
認証データ送信要求の受信
S404
{KPm3//Cm3}KPaを出力
S406
{KPm3//Cm3}KPaを
受信側から受理し、送信側に入力
S408
{KPm3//Cm3}KPaを受理し
KPaにて復号
S410
KPm3の
受理
S412
No
Yes
セッション鍵Ks2cの生成
S414
Ks2cをKPm3にて暗号化し、
{Ks2c}Km3の出力
S416
{Ks2c}Km3を送信側から受理
S418
{Ks2c}Km3
を受信側に入力
S420
{Ks2c}Km3を受理し、Km3にて復号
Ks2cの受理
S422
受信ログよりKs2bを取得し、Ks2cにて暗号化
{Ks2b}Ks2cの生成
S424
受信ログよりライセンスID、受信stateを取得し、
ライセンスID//{Ks2b}Ks2c//受信state
のハッシュ値hashを求める
S426
hashをKs2cにて暗号化
{hash}Ks2cの生成
S428
ライセンスID//{Ks2b}Ks2c//受信state//{hash}Ks2c
を出力
S430
受信stateの
確認
S432
OFF
ON
ライセンスIDの確認
S434
不一致
一致
ライセンスID//{Ks2b}Ks2c//受信state//{hash}Ks2c
を受信側から受理し、送信側へ入力
S436
S438へ
S462へ

FIG.19

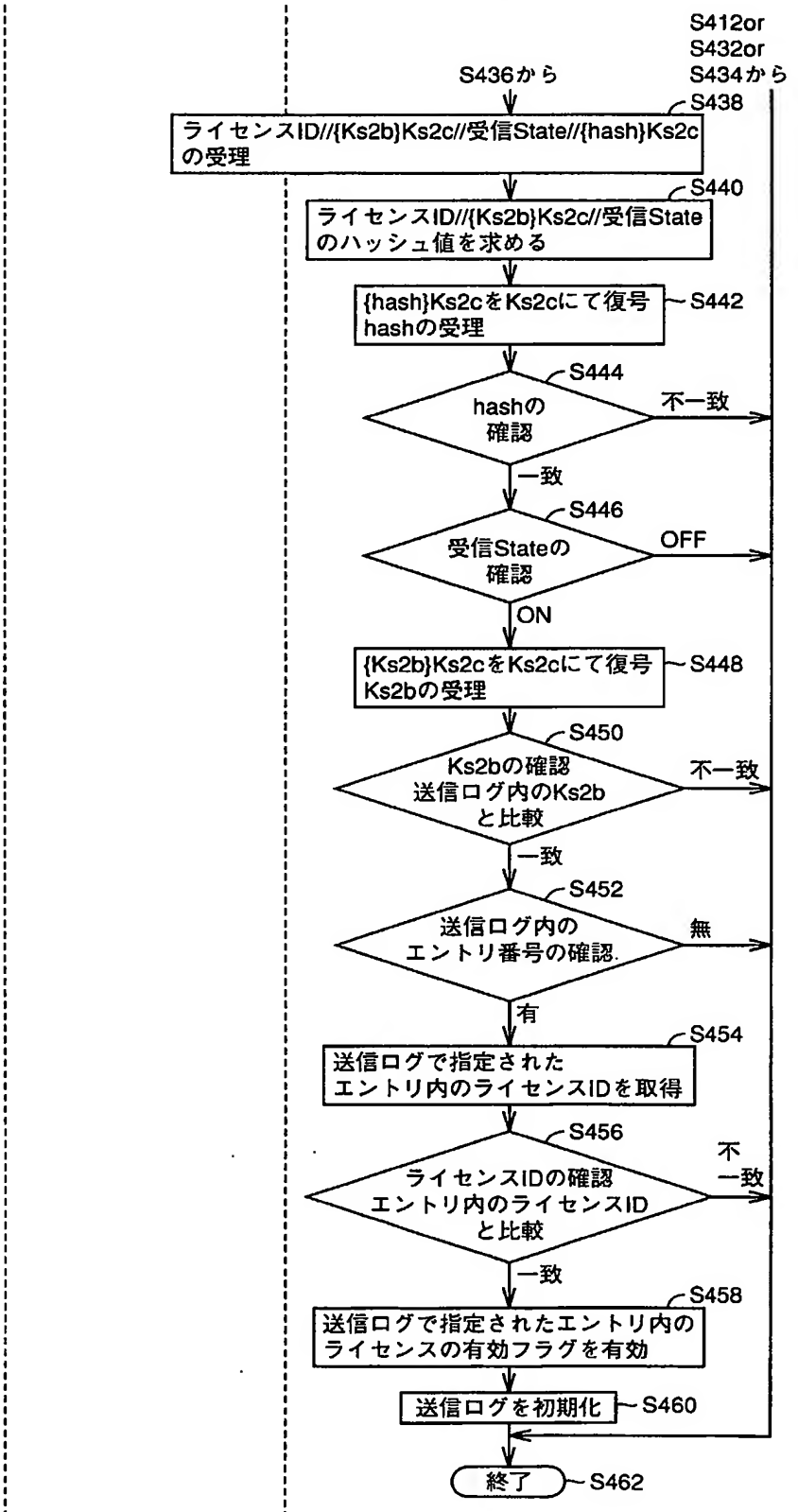
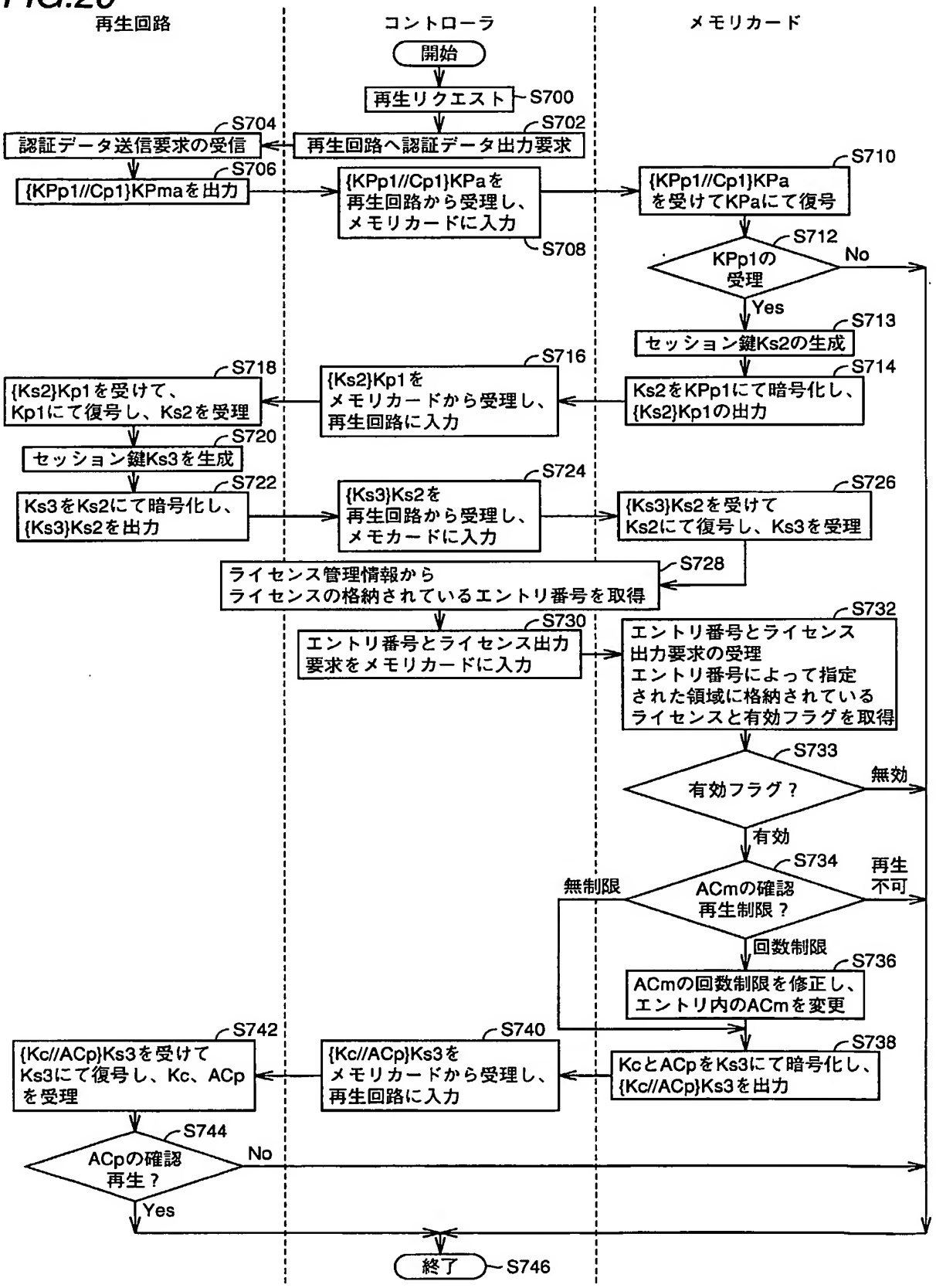

受信側
メモリカード110
コントローラ
送信側
メモリカード120
S412or
S432or
S434から
S436から
S438
ライセンスID//{Ks2b}Ks2c//受信State//{hash}Ks2c
の受理
S440
ライセンスID//{Ks2b}Ks2c//受信State
のハッシュ値を求める
{hash}Ks2cをKs2cにて復号
hashの受理
S442
S444
hashの
確認
不一致
一致
S446
受信Stateの
確認
OFF
ON
{Ks2b}Ks2cをKs2cにて復号
Ks2bの受理
S448
S450
Ks2bの確認
送信ログ内のKs2b
と比較
不一致
一致
S452
送信ログ内の
エントリ番号の確認
無
有
S454
送信ログで指定された
エントリ内のライセンスIDを取得
S456
ライセンスIDの確認
エントリ内のライセンスID
と比較
不
一致
一致
S458
送信ログで指定されたエントリ内の
ライセンスの有効フラグを有効
送信ログを初期化
S460
終了
S462

FIG.20


再生回路
コントローラ
メモリカード
開始
再生リクエスト
S700
再生回路へ認証データ出力要求
S702
認証データ送信要求の受信
S704
{KPp1//Cp1}KPmaを出力
S706
{KPp1//Cp1}KPaを
再生回路から受理し、
メモリカードに入力
S708
{KPp1//Cp1}KPa
を受けてKPaにて復号
S710
KPp1の
受理
S712
No
Yes
セッション鍵Ks2の生成
S713
Ks2をKPp1にて暗号化し、
{Ks2}Kp1の出力
S714
{Ks2}Kp1を
メモリカードから受理し、
再生回路に入力
S716
{Ks2}Kp1を受けて、
Kp1にて復号し、Ks2を受理
S718
セッション鍵Ks3を生成
S720
Ks3をKs2にて暗号化し、
{Ks3}Ks2を出力
S722
{Ks3}Ks2を
再生回路から受理し、
メモカードに入力
S724
{Ks3}Ks2を受けて
Ks2にて復号し、Ks3を受理
S726
ライセンス管理情報から
ライセンスの格納されているエントリ番号を取得
S728
エントリ番号とライセンス出力
要求をメモリカードに入力
S730
エントリ番号とライセンス
出力要求の受理
エントリ番号によって指定
された領域に格納されている
ライセンスと有効フラグを取得
S732
有効フラグ？
S733
無効
有効
ACmの確認
再生制限？
S734
無制限
再生
不可
回数制限
ACmの回数制限を修正し、
エントリ内のACmを変更
S736
KcとACpをKs3にて暗号化し、
{Kc//ACp}Ks3を出力
S738
{Kc//ACp}Ks3を
メモリカードから受理し、
再生回路に入力
S740
{Kc//ACp}Ks3を受けて
Ks3にて復号し、Kc、ACp
を受理
S742
ACpの確認
再生？
S744
No
Yes
終了
S746

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP01/07862

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06F15/00, G06F17/60

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06F15/00, G06F17/60

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Kokai Jitsuyo Shinan Koho 1971-2001
Jitsuyo Shinan Toroku Koho 1996-2001 Toroku Jitsuyo Shinan Koho 1994-2001

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2000-305853 A (Victor Company of Japan, Limited), 02 November, 2000 (02.11.00), & EP 1047062 A2	1-16
A	JP 2000-285028 A (Minolta Co., Ltd.), 13 October, 2000 (13.10.00), Par. Nos. [0029] to [0034] (Family: none)	1-16
A	JP 2001-051906 A (Sony Corporation), 23 February, 2001 (23.02.01), (Family: none)	1-16
A	JP 2001-014221 A (Victor Company of Japan, Limited), 19 January, 2001 (19.01.01), (Family: none)	1-16
A	JP 2001-022859 A (Victor Company of Japan, Limited), 26 January, 2001 (26.01.01), (Family: none)	1-16

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
03 December, 2001 (03.12.01)	11 December, 2001 (11.12.01)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)

国際調査報告

国際出願番号　PCT／JP01／07862

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　G06F12／14, G06F15／00, G06F17／60

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　G06F12／14, G06F15／00, G06F17／60

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996
日本国実用新案登録公報	1996－2001
日本国公開実用新案公報	1971－2001
日本国登録実用新案公報	1994－2001

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
A	JP　2000－305853　A（日本ビクター株式会社）2．11月．2000（02．11．00），&EP　1047062　A2	1－16
A	JP　2000－285028　A（ミノルタ株式会社）13．10月．2000（13．10．00），段落29ないし段落34（ファミリーなし）	1－16
A	JP　2001－051906　A（ソニー株式会社）23．2月．2001（23．02．01），（ファミリーなし）	1－16
A	JP　2001－014221　A（日本ビクター株式会社）19．1月．2001（19．01．01），（ファミリーなし）	1－16

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日　03．12．01	国際調査報告の発送日　11.12.01
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員） 梅村　勁樹　印 5N　7313 電話番号　03－3581－1101　内線　3545

様式PCT／ISA／210（第2ページ）（1998年7月）

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ０１／０７８６２

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ａ	ＪＰ　２００１－０２２８５９　Ａ（日本ビクター株式会社）２６．１月．２００１（２６．０１．０１），（ファミリーなし）	１－１６